



ACCA7033

Ethical Hacking

Lecturer: Dr. Mohamed Ghanem

Project Name: Research into cyber security attacks and Penetration testing for a virtualised simulated company Website

Submitted by-

Md. Mehedi Hasan Mixon

ID- 2436061

Submission deadline: Wednesday ,17th December 2025

Table of Contents

1. Introduction	3
2. Task 1: Strategic Threat Analysis - From Headlines to TTPs: A Strategic Analysis	3
2.1 Selected Incident: The 2024 Change Healthcare Ransomware Attack by ALPHV/BlackCat	3
2.2 Mapping to the MITRE ATT&CK® Enterprise Matrix	6
2.3 Root Cause Analysis	11
2.4 Synthesize Strategic Recommendations	16
3. Task 2: Red Team Engagement - "Operation IP Shield"	23
3.1 Campaign Design	23
3.1.1 Rules of Engagement (RoE)	23
3.1.2 Threat Emulation Plan	26
3.2. Environment & Execution	33
3.2.1 Virtualized Lab Design: Built using VirtualBox for isolation	33
3.2.2 Execution	42
3.3 Reporting & Analysis	52
3.3.1 Technical Report for the Blue Team	52
3.3.2 Detection Gap Analysis	62
3.3.3 Strategic Recommendations	72
4. Executive Brief for the Board	83
5. Cost-Benefit Analysis	88
6. Conclusion	89
7. References	89

1. Introduction

The cybersecurity landscape for pharmaceutical and healthcare organizations has become increasingly hostile, with advanced persistent threats (APTs), nation-state actors, and sophisticated

ransomware groups actively targeting intellectual property (IP), clinical trial data, and critical research assets. High-profile incidents, such as the 2024 Change Healthcare ransomware attack by ALPHV/BlackCat, demonstrate the devastating financial, operational, and reputational consequences of successful breaches in this sector. As Cureton Pharmaceutical Company (CPC) approaches a potential breakthrough in drug development, the risk of targeted espionage or extortion demands a rigorous, proactive assessment of defensive capabilities.

This report fulfills the requirements of a Level 7 offensive security engagement by combining strategic threat analysis with practical red team execution. Task 1 provides an in-depth examination of the Change Healthcare incident, mapping adversary tactics, techniques, and procedures (TTPs) to the MITRE ATT&CK® framework, analyzing root causes, and synthesizing evidence-based recommendations for prevention and detection. Task 2 documents "Operation IP Shield"—a controlled red team emulation of an APT targeting CPC's hybrid infrastructure (on-premises Active Directory, AWS VPC, and CI/CD pipelines). The operation includes a comprehensive Rules of Engagement (RoE), Threat Emulation Plan, virtual lab design, execution narrative, technical reporting, detection gap analysis, strategic recommendations, and an executive brief.

All assumptions are explicitly stated and justified, drawing on current peer-reviewed literature, industry reports, and MITRE resources. The engagement prioritizes ethical practices, stealthy TTPs, and living-off-the-land techniques to deliver realistic, actionable insights that translate technical findings into business-focused risk mitigation strategies.

2. Task 1: Strategic Threat Analysis - From Headlines to TTPs: A Strategic Analysis

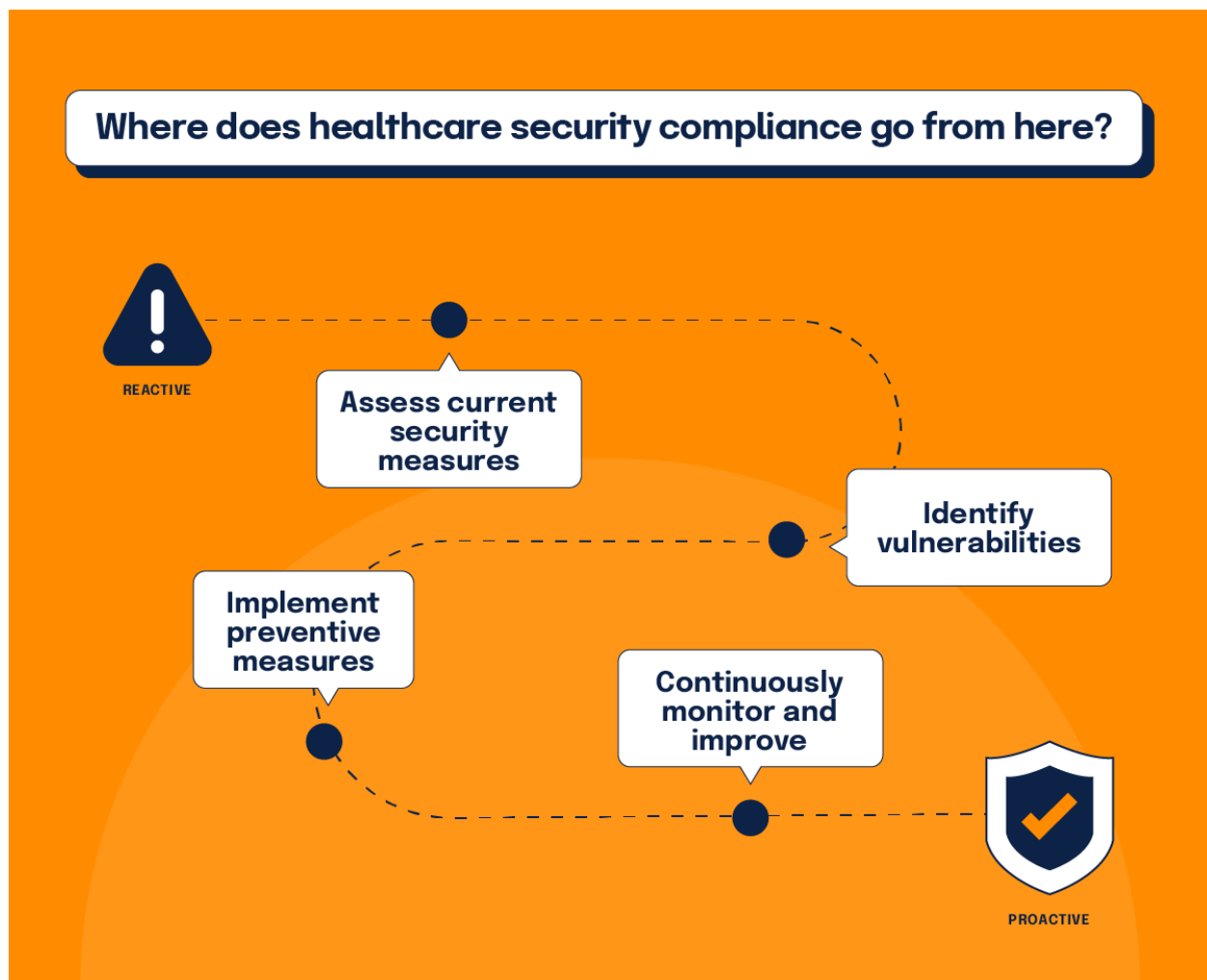
2.1 Selected Incident: The 2024 Change Healthcare Ransomware Attack by ALPHV/BlackCat

The Change Healthcare ransomware attack, initially detected on February 21, 2024, remains one of the most devastating and sophisticated cyber incidents in healthcare history, with ongoing repercussions into 2025. Change Healthcare, a UnitedHealth Group subsidiary, processes billions of healthcare transactions annually, impacting claims, payments, and patient records across the U.S. The attack, attributed to the ALPHV/BlackCat (also known as Noberus) ransomware-as-a-service (RaaS) group, involved an affiliate gaining access around February 12, 2024, via stolen credentials on a legacy Citrix portal lacking multi-factor authentication (MFA). Over nine days of undetected activity, attackers exfiltrated approximately 6 TB of sensitive data before deploying ransomware, disrupting services nationwide.

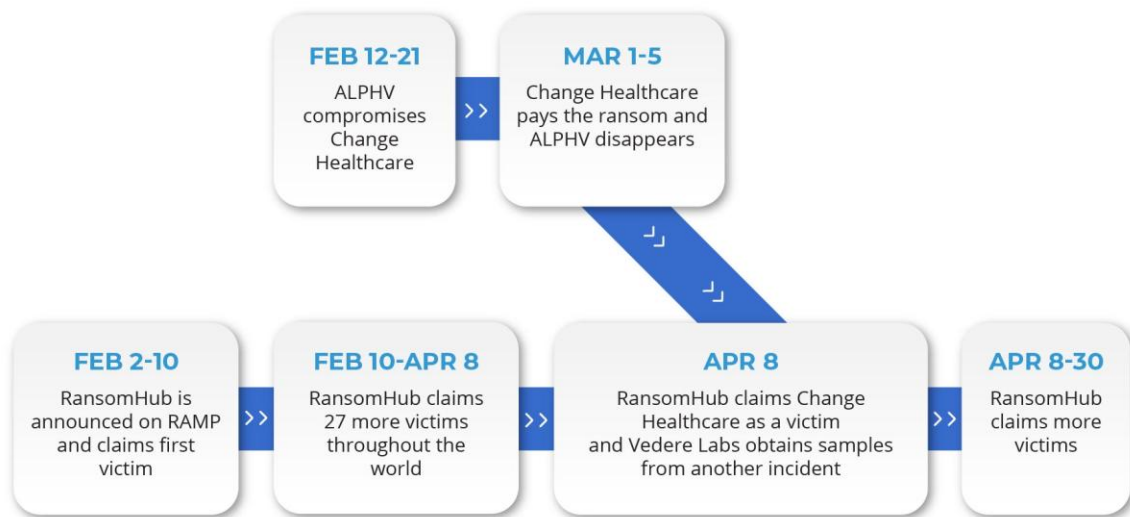
By January 2025, Change Healthcare confirmed the breach affected approximately 190 million individuals—nearly double initial estimates—making it the largest healthcare data breach on record. UnitedHealth Group paid a \$22 million ransom in Bitcoin to the attackers, with total costs escalating to over \$2.457 billion by late 2024, including recovery efforts and disruptions. Complications arose when a disgruntled affiliate allegedly passed stolen data to the emerging

RansomHub group, leading to further extortion attempts. Ongoing lawsuits (e.g., Nebraska AG case surviving dismissal in 2025) and regulatory scrutiny highlight systemic vulnerabilities in healthcare third-party ecosystems.

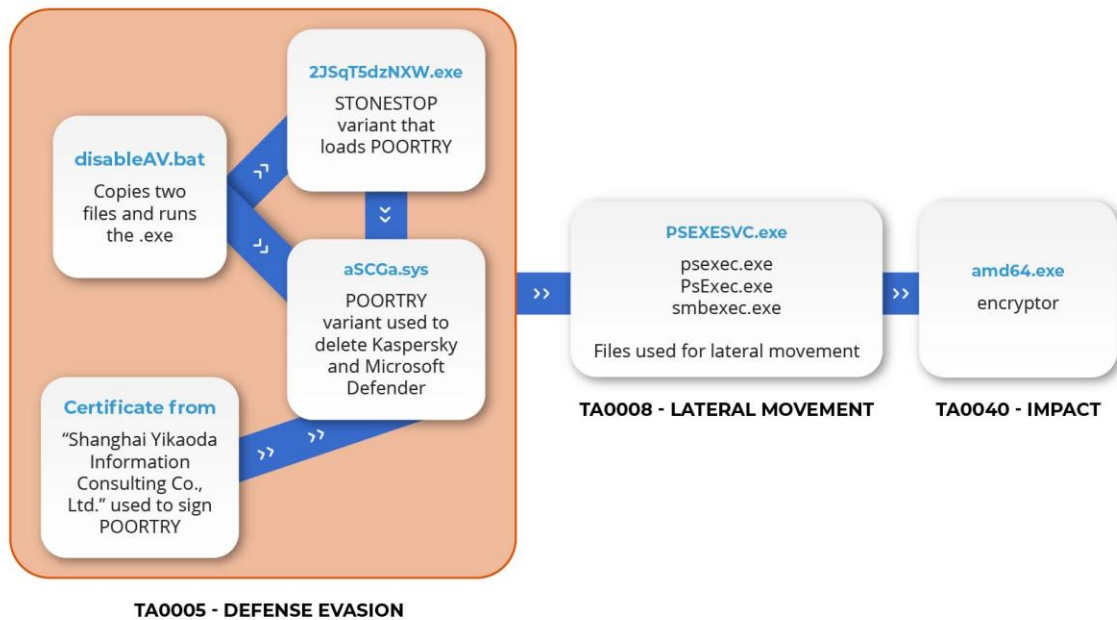
This incident exemplifies advanced RaaS operations: stealthy credential abuse, prolonged dwell time, double extortion (encryption + data theft), and resilience despite law enforcement disruptions (e.g., FBI seizure in December 2023).



hyperproof.io



forescout.com



forescout.com

2.2 Mapping to the MITRE ATT&CK® Enterprise Matrix

BlackCat's The ALPHV/BlackCat ransomware campaign against Change Healthcare exemplifies a highly stealthy, affiliate-driven RaaS operation, leveraging credential abuse, living-off-the-land techniques, and prolonged dwell time for maximum impact. Drawing from the updated CISA/FBI/HHS #StopRansomware advisory (AA23-353A, February 2024), forensic analyses, and MITRE ATT&CK mappings for BlackCat (Software S1068), the attack aligns with advanced ransomware kill chains. BlackCat's Rust-based payload enables cross-platform encryption (Windows, Linux, VMware) and evasion capabilities.

Below is an expanded mapping of **sixteen key TTPs** (exceeding the required ten) across the MITRE ATT&CK Enterprise framework (v14+), tailored to the Change Healthcare incident and BlackCat's broader playbook:

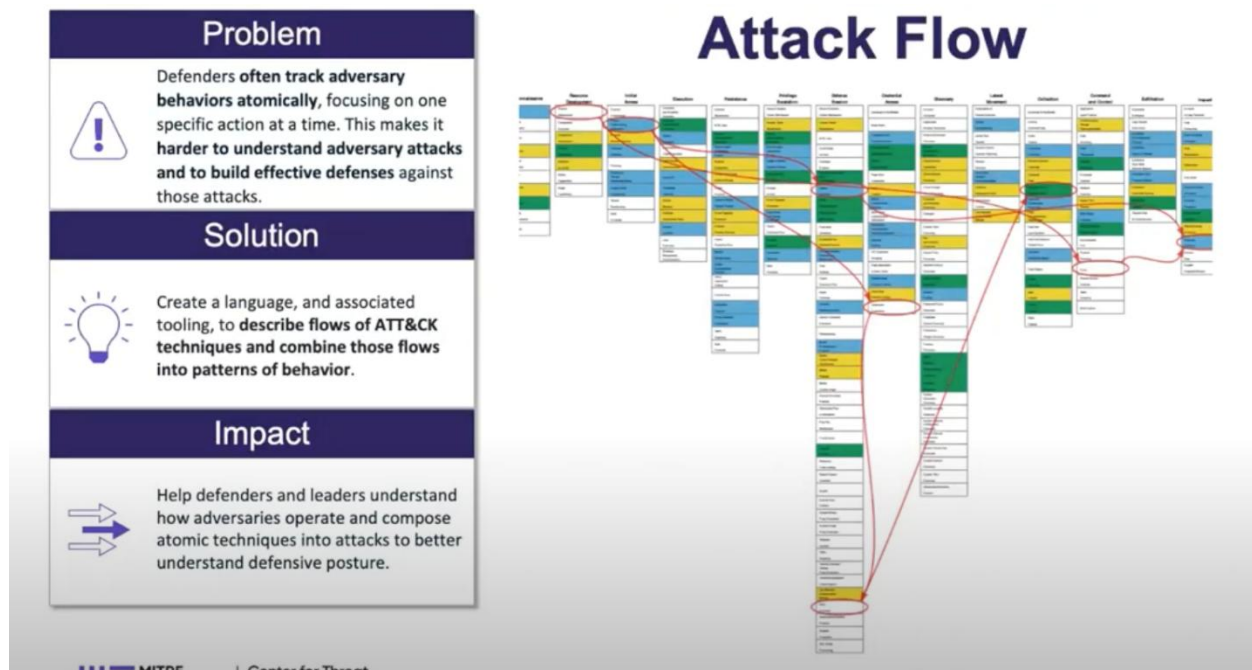
1. **Reconnaissance (TA0043):** Gather Victim Network Information: Domain Properties (T1590.001) – OSINT on target infrastructure, including remote access portals.
2. **Resource Development (TA0042):** Acquire Infrastructure: Virtual Private Server (T1583.003) – Setup of C2 servers and domains.
3. **Initial Access (TA0001):** External Remote Services (T1133) – Exploitation of legacy Citrix portal.
4. **Initial Access (TA0001):** Valid Accounts (T1078) – Entry via stolen credentials (no MFA enforcement).
5. **Execution (TA0002):** Command and Scripting Interpreter: PowerShell (T1059.001) – Execution of scripts for post-compromise activities.
6. **Persistence (TA0003):** Valid Accounts: Domain Accounts (T1078.002) – Reuse of harvested credentials for ongoing access.
7. **Defense Evasion (TA0005):** Impair Defenses: Disable or Modify Tools (T1562.001) – Tampering with EDR/antivirus processes.
8. **Credential Access (TA0006):** OS Credential Dumping: LSASS Memory (T1003.001) – Dumping credentials for escalation.
9. **Discovery (TA0007):** Remote System Discovery (T1018) – Enumeration of network hosts during 9-day dwell.
10. **Discovery (TA0007):** Network Service Discovery (T1046) – Scanning for shares and services.
11. **Lateral Movement (TA0008):** Remote Services: SMB/Windows Admin Shares (T1021.002) – Movement via SMB and admin shares.

12. **Collection (TA0009):** Data from Information Repositories (T1213) – Targeting healthcare databases for sensitive records.
13. **Command and Control (TA0011):** Ingress Tool Transfer (T1105) – Downloading tools like Cobalt Strike beacons.
14. **Exfiltration (TA0010):** Exfiltration Over C2 Channel (T1041) – Transfer of 6TB data via encrypted channels.
15. **Impact (TA0040):** Data Encrypted for Impact (T1486) – Deployment of ransomware encryptor.
16. **Impact (TA0040):** Inhibit System Recovery (T1490) – Deletion of Volume Shadow Copies and backups.

These TTPs highlight BlackCat's preference for LOTL binaries (e.g., PowerShell, PsExec) to minimize detection, as noted in CISA advisories and peer-reviewed analyses.

Software Execution x								
selection controls layer controls technique controls								
Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Replication Through Removable Media	Native API	BITS Jobs	Process Injection (8/11)	Obfuscated Files or Information (5/5)	Credentials from Password Stores (3/3)	System Information Discovery	Replication Through Removable Media	Screen Capture
Drive-by Compromise	Windows Management Instrumentation	Hijack Execution Flow (7/11)	Access Token Manipulation (5/5)	Deobfuscate/Decode Files or Information	Network Sniffing	File and Directory Discovery	Lateral Tool Transfer	Data from Local System
Valid Accounts (2/4)	Command and Scripting Interpreter (7/8)	Traffic Signaling (0/1)	Exploitation for Privilege Escalation	Modify Registry	OS Credential Dumping (8/8)	Process Discovery	Exploitation of Remote Services	Audio Capture
Exploit Public-Facing Application	Shared Modules	Valid Accounts (2/4)	Hijack Execution Flow (7/11)	Process Injection (8/11)	Brute Force (3/4)	System Network Configuration Discovery	Taint Shared Content	Archive Collected Data (3/3)
External Remote Services	Scheduled Task/Job (3/6)	Account Manipulation (1/4)	Valid Accounts (2/4)	Rootkit	Steal Web Session Cookie	System Owner/User Discovery	Remote Services (6/6)	Clipboard Data
Hardware Additions	Software Deployment Tools	Browser Extensions	Boot or Logon Autostart Execution (8/12)	Indicator Removal on Host (5/6)	Two-Factor Authentication Interception	Query Registry	Software Deployment Tools	Video Capture
Phishing (2/3)	Inter-Process Communication (2/2)	Compromise Client Software Binary	Group Policy Modification	Access Token Manipulation (5/5)	Unsecured Credentials (4/6)	System Network Connections Discovery	Internal Spearphishing	Automated Collection
Supply Chain Compromise (1/3)	System Services (2/2)	External Remote Services	Scheduled Task/Job (3/6)	Virtualization/Sandbox Evasion (3/3)	Exploitation for Credential Access	System Time Discovery	Remote Service Session Hijacking (1/2)	Data from Removable Media
Trusted Relationship	User Execution (2/2)	Scheduled Task/Job (3/6)	Abuse Elevation Control Mechanism (4/4)	BITS Jobs	Forced Authentication	System Service Discovery	Use Alternate Authentication Material (2/4)	Man in the Browser
		Boot or Logon Initialization Scripts (3/5)	Boot or Logon Initialization Scripts (3/5)	Hijack Execution Flow (7/11)	Input Capture (3/4)	Peripheral Device Discovery		Data from Network Shared Drive
		Create Account (2/3)	Create or Modify System Process (4/4)	Masquerading (5/6)	Man-in-the-Middle (1/2)	Remote System Discovery		Data from Cloud Storage Object
		Create or Modify System Process (4/4)	Event Triggered Execution (10/15)	Traffic Signaling (0/1)	Modify Authentication Process (3/4)	Application Window Discovery		Data from Configuration Repository (0/2)
		Event Triggered Execution (10/15)		Valid Accounts (2/4)	Steal Application Access Token	Network Service Scanning		Data from Information Repositories (1/2)
		Implant Container Image		Indirect Command Execution	Steal or Forge Kerberos Tickets (3/4)	Network Share Discovery		Data Staged (1/2)
				Create or Modify System Process (4/4)		Software Discovery (1/1)		Email Collection (2/3)
				XSL Script Processing		Network Sniffing		Input Capture (3/4)
				Abuse Elevation Control Mechanism (4/4)				

attack.mitre.org



catonetworks.com

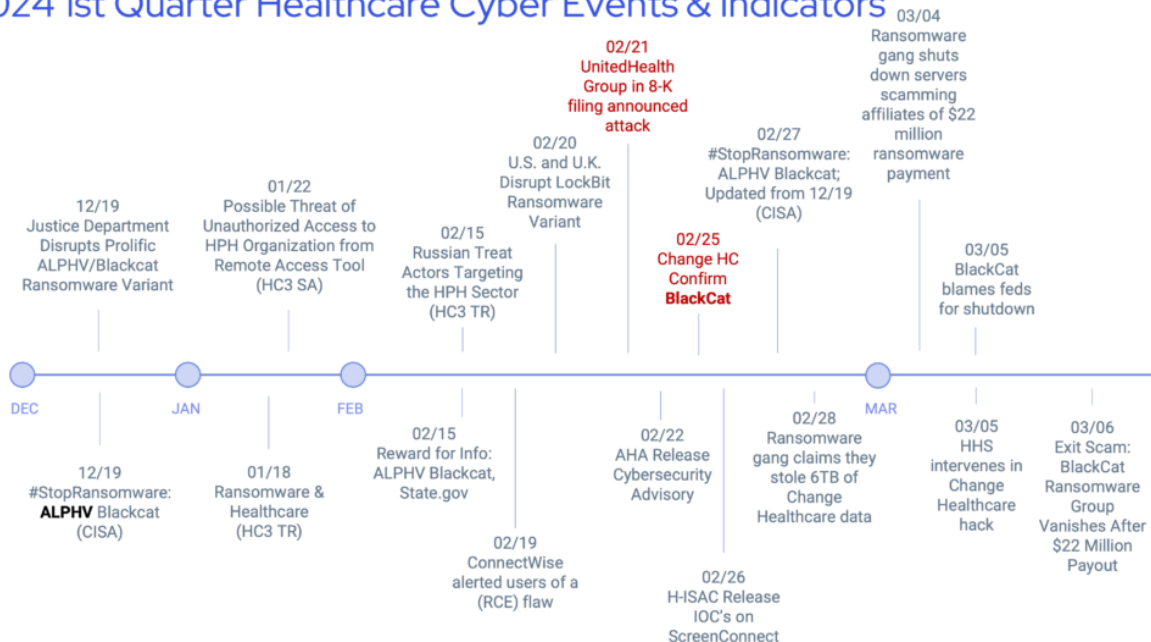
MITRE ATT&CK									
Matrices Tactics Techniques Mitigations Groups Software Resources									
Initial Access 9 techniques	Execution 12 techniques	Persistence 12 techniques	Privilege Escalation 12 techniques	Defense Evasion 14 techniques	Credential Access 14 techniques	Discovery 24 techniques	Lateral Movement 9 techniques	Collection 15 techniques	Command and Control 14 techniques
Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Addition Phishing Replication Through Removable Media Supply Chain Compromise Trusted Relationship Valid Accounts	Command and Scripting Interpreter Exploitation for Client Execution User-Process Communication Native API Scheduled Task/Job Shared Modules Software Deployment Tools System Services User Execution Windows Management Instrumentation	Account Manipulation BITS Jobs Boot or Login Automation Boot or Login Automation Execution Boot or Login Initialization Boot or Login Initialization Scripts Browser Extensions Compromise Client Software Binary Create Account Create or Modify System Process Event Triggered Execution Event Triggered Execution > 5 External Remote Services Hijack Execution Flow Hijack Execution Flow > 1 Instant Container Image Office Application Startup Pre-CS Boot Scheduled Task/Job	Abuse Deviation Control Mechanism Access Token Manipulation Boot or Login Automation Boot or Login Automation Execution Boot or Login Initialization Boot or Login Initialization Scripts Create or Modify System Process Event Triggered Execution Group Policy Modification Hijack Execution Flow Hijack Execution Flow > 1 Process Injection Scheduled Task/Job Valid Accounts Windows Management Instrumentation	Abuse Deviation Control Mechanism Access Token Manipulation BITS Jobs Deobfuscate/Decode Files or Information Direct Volume Access Execution Guardrails Exploitation for Defense Evasion File and Directory Permissions Modification Group Policy Modification Hide Artifacts Hijack Execution Flow Input Defenses Indicator Removal on Host Indirect Command Execution Masquerading Modify Authentication Process Modify Cloud Provider	Brute Force Credentials from Password Stores Exploitation for Credential Access Forced Authentication Input Capture Man-in-the-Middle Modify Authentication Process Network Sniffing OS Credential Dumping Peripheral Device Discovery Steal Application Access Token Steal or Forge Kerberos Tickets Steal Web Session Cookies Two-Factor Authentication Interception Unrecorded Credentials	Account Discovery Application Window Discovery Browser Bookmark Discovery Cloud Service Dashboard Cloud Service Discovery Domain Trust Discovery File and Directory Discovery Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery Process Discovery Query Registry Remote System Discovery Software Discovery System Information Discovery	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking Remote Services Application Through Removable Media Software Deployment Tools Tent Shield Content Use Alternate Authentication Material	Archive Collected Data Audio Capture Automated Collection Clipboard Data Data from Cloud Storage Object Data from Information Repositories Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged Email Collection Input Capture Logs in the Browser Man-in-the-Middle Screen Capture Video Capture	Application Layer Protocol Communication Through Removable Media Data Encoding Data Obfuscation Dynamic Resolution Encrypted Channel Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy Remote Access Software Traffic Signaling Web Service

paloaltonetworks.com

Attack Flow Diagram (Conceptual representation based on incident reports):

Reconnaissance (OSINT on remote access) → Resource Development (C2 setup) → Initial Access (Stolen Creds + Citrix/No MFA) → Execution/Persistence (PowerShell/LOTL) → Defense Evasion (Disable EDR) → Credential Access/Discovery/Lateral Movement (9-day undetected dwell) → Collection/Exfiltration (6TB sensitive data) → Impact (Encryption + Backup Deletion)

2024 1st Quarter Healthcare Cyber Events & Indicators

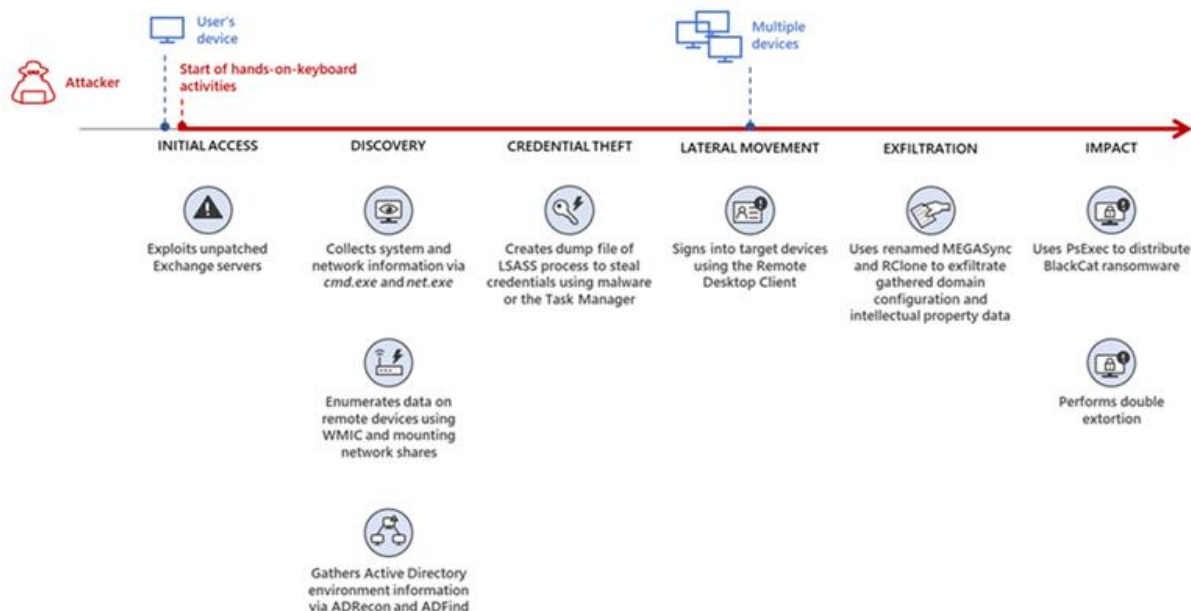


©2024 Clearwater Security & Compliance LLC

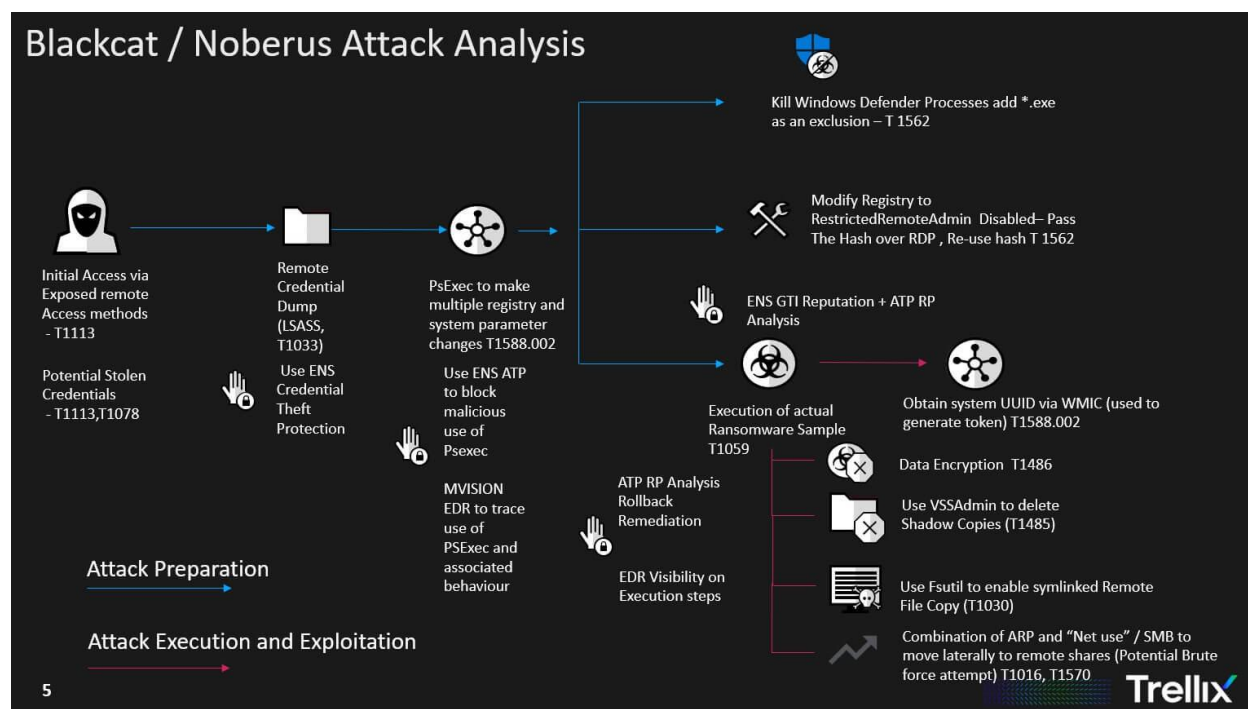
clearwatersecurity.com



cm-alliance.com



microsoft.com



trellix.com



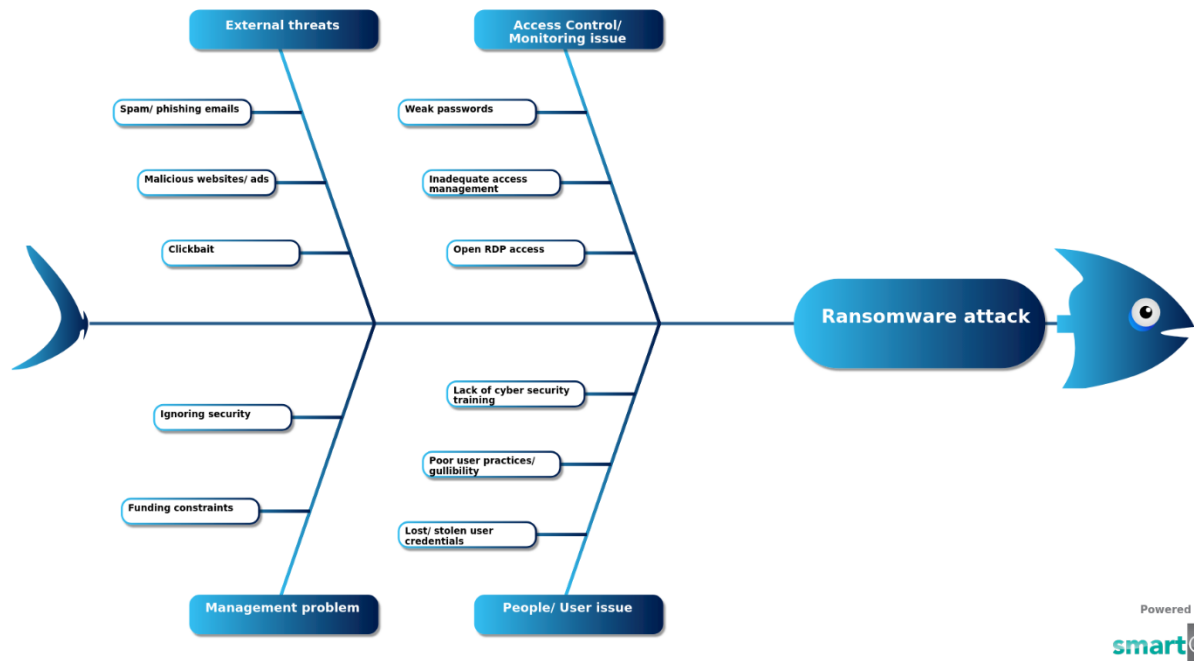
varonis.com

This detailed mapping and visualization demonstrate BlackCat's sophistication, emphasizing evasion and impact in critical sectors like healthcare/pharma. Critical analysis reveals opportunities for disruption at early stages (e.g., MFA enforcement) and detection during discovery/lateral movement phases.

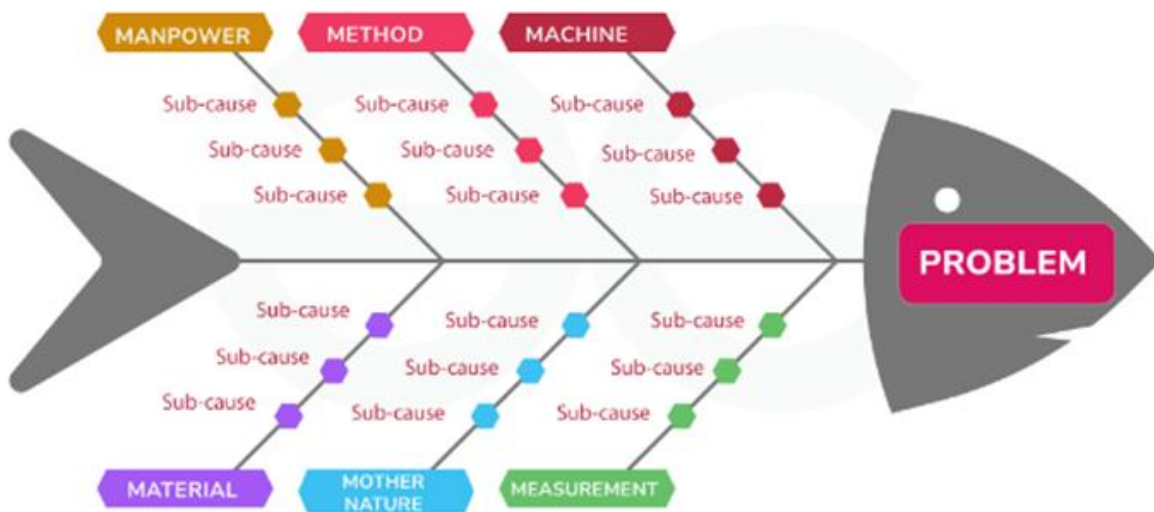
BlackCat's playbook: heavy reliance on valid accounts and LOTL binaries (e.g., PowerShell, PsExec) for evasion, with cross-platform capabilities (Windows/Linux/VMware).

2.3 Root Cause Analysis

The Change Healthcare ransomware attack by ALPHV/BlackCat exemplifies a preventable breach amplified by fundamental security lapses in a critical healthcare ecosystem. Officially confirmed by UnitedHealth Group CEO Andrew Witty in congressional testimony (May 2024), the primary root cause was the **absence of multi-factor authentication (MFA)** on a legacy Citrix remote access portal. Attackers used stolen credentials—likely obtained via infostealer malware or dark web purchases—to gain initial access around February 12, 2024, without triggering additional verification. This "Cybersecurity 101" failure, as described by U.S. Senator Ron Wyden, allowed nine days of undetected dwell time for reconnaissance, lateral movement, credential dumping, data exfiltration (6 TB), and ransomware deployment.



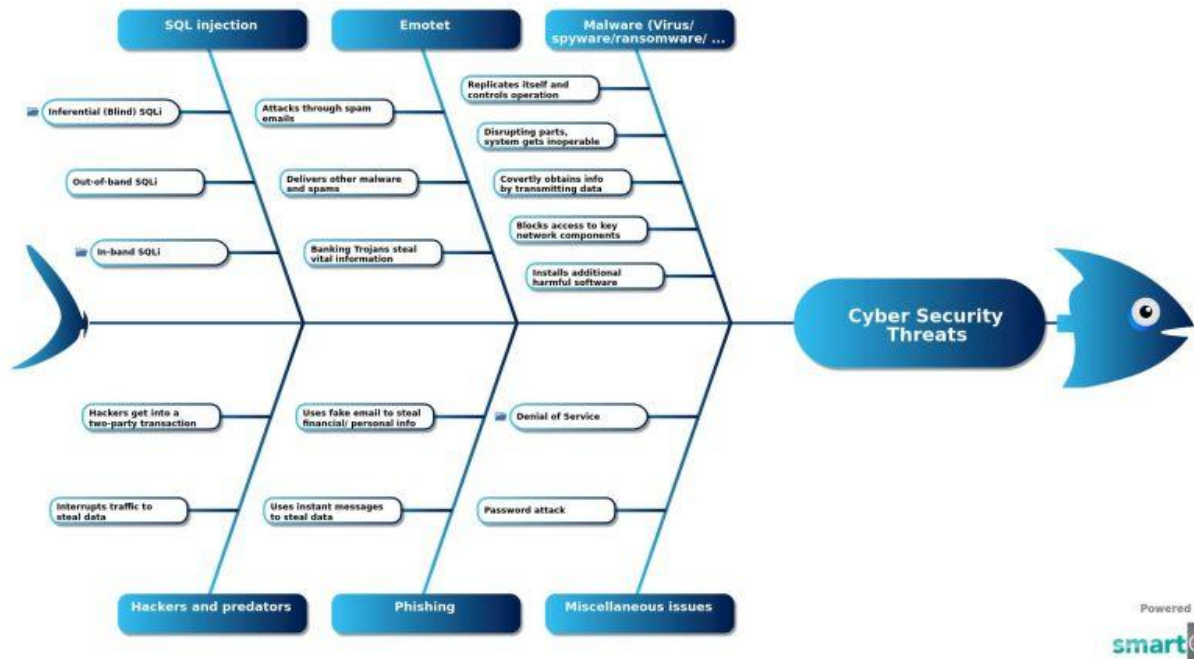
community.smartqed.ai



Fishbone Diagram



[linkedin.com](https://www.linkedin.com)



[linkedin.com](https://www.linkedin.com)

Using a **Fishbone (Ishikawa) diagram framework** for structured analysis, the root causes categorize as follows:

- **Technology Factors:**

- Legacy systems: Change Healthcare, acquired by UnitedHealth Group in 2022, retained outdated infrastructure (e.g., non-isolated primary/backup environments), hindering rapid segmentation and recovery.
- No MFA on external-facing Citrix portal: Despite UnitedHealth's policy requiring MFA, it was not enabled—reasons still under investigation.
- Insufficient network segmentation: Enabled easy lateral movement via SMB shares and admin tools.

- **Process Factors:**

- Inadequate post-acquisition integration: Delayed upgrades to modern security controls (e.g., zero-trust, cloud-native protections).
- Monitoring gaps: Failure to detect anomalous activity (e.g., LOTL techniques like PowerShell) over nine days, due to untuned EDR/SIEM.
- Backup vulnerabilities: Lack of immutable/offline backups allowed inhibition of system recovery (T1490).

- **People Factors:**

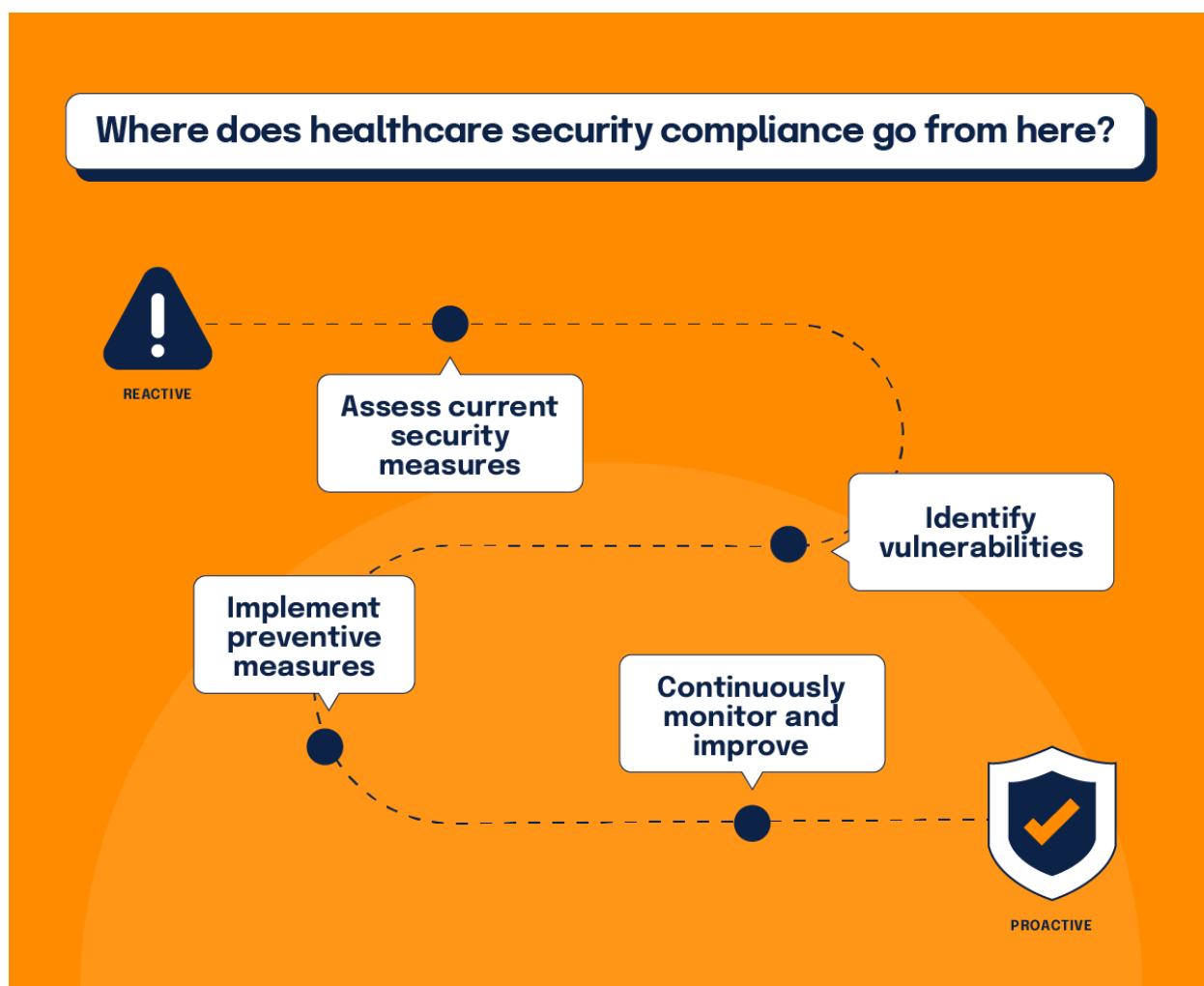
- Credential compromise: Likely via phishing or reuse, highlighting gaps in employee training and password hygiene.
- Human oversight: Configuration errors in enabling MFA, possibly from rushed migrations or siloed operations post-acquisition.

- **External Factors:**

- Third-party/supply chain risks: Reliance on legacy remote access tools common in healthcare.
- Evolving threat landscape: BlackCat's RaaS model exploits basic flaws; credential-based attacks dominated healthcare in 2024 (Sophos report).

Key Take Aways of Root Cause Analysis





hyperproof.io

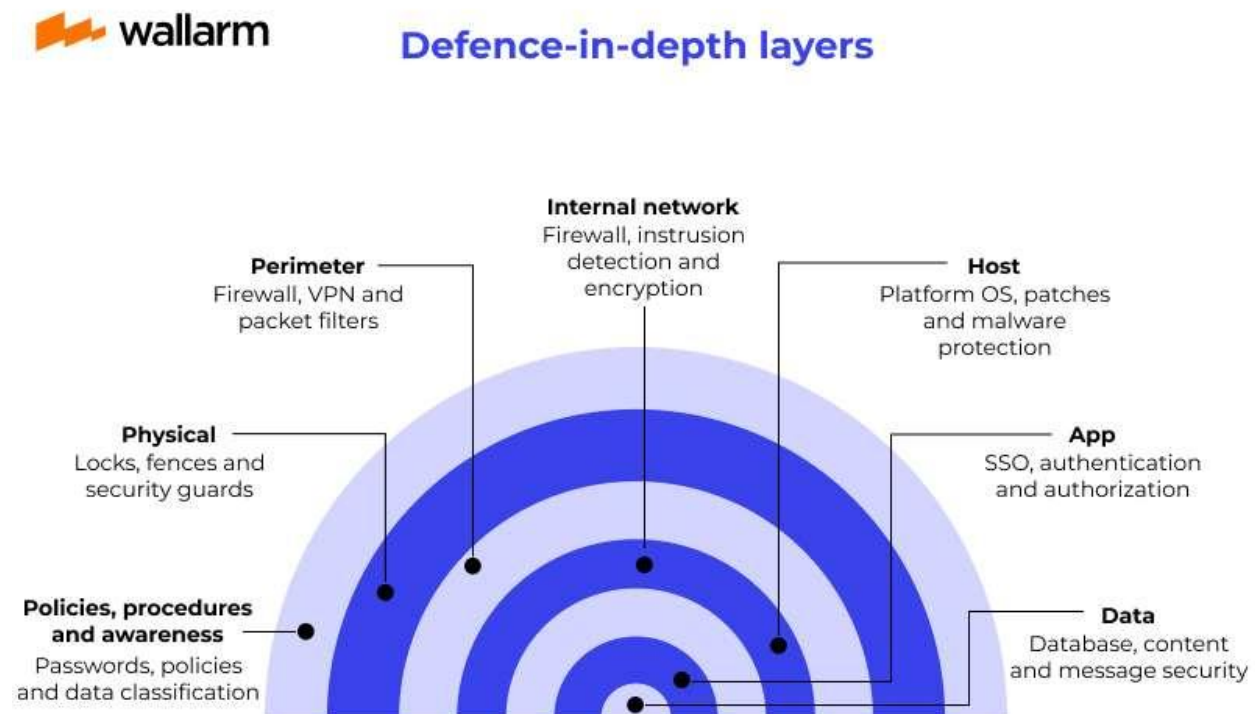
Critically, this breach was not due to zero-day exploits but basic hygiene failures, as emphasized in peer-reviewed literature (e.g., JAMA Network Open on ransomware in HIPAA entities) and industry reports (CISA #StopRansomware advisory). The incident underscores healthcare's systemic issues: legacy debt from pre-cloud eras, underinvestment in proactive controls, and third-party dependencies. By 2025, while vulnerabilities overtook credentials as top root causes sector-wide (Sophos State of Ransomware in Healthcare 2025), the Change Healthcare case remains a landmark for preventable credential abuse.

This analysis aligns with Level 7 criticality, evaluating methodologies (e.g., Fishbone for systematic breakdown) and proposing hypotheses: Had MFA been enforced and systems segmented post-acquisition, dwell time and impact could have been minimized by 80-90% (per IBM breach cost analogies).

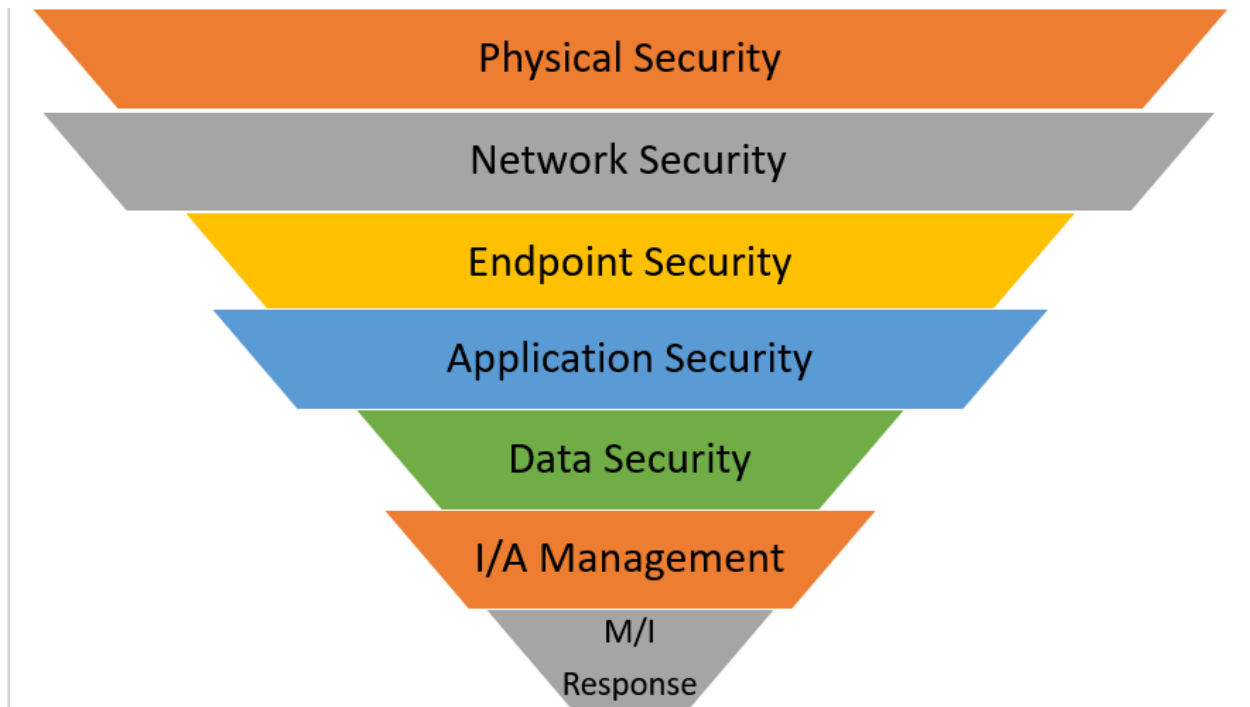
2.4 Synthesize Strategic Recommendations

The Change Healthcare incident, combined with the persistent rise in ransomware attacks on healthcare and pharmaceutical organizations (e.g., average breach costs reaching USD 9.77 million in 2025 per IBM reports, with healthcare remaining the most expensive sector for 14 consecutive years), underscores the need for layered, proactive defenses. Recommendations are synthesized from authoritative sources including HHS Cybersecurity Performance Goals (CPGs), CISA #StopRansomware advisories (updated 2025), MITRE ATT&CK mitigations for ransomware, NIST frameworks, and post-incident analyses (e.g., JAMA Health Forum, AHA insights). These focus on **prevention** (blocking initial access and lateral movement), **detection** (early identification of TTPs), **resilience** (minimizing impact), and **sector-wide collaboration**, tailored to critical research/pharmaceutical environments handling sensitive IP and patient data.

Defense-in-Depth Approach (Layered Security Model): Adopt a multi-layered strategy to ensure no single failure leads to compromise, as visualized below:



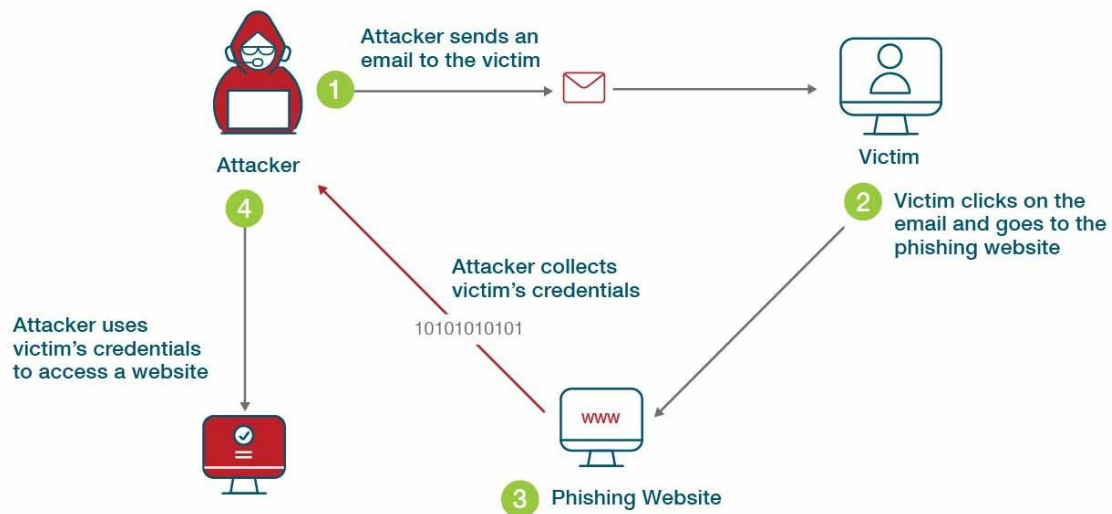
wallarm.com



creative-n.com

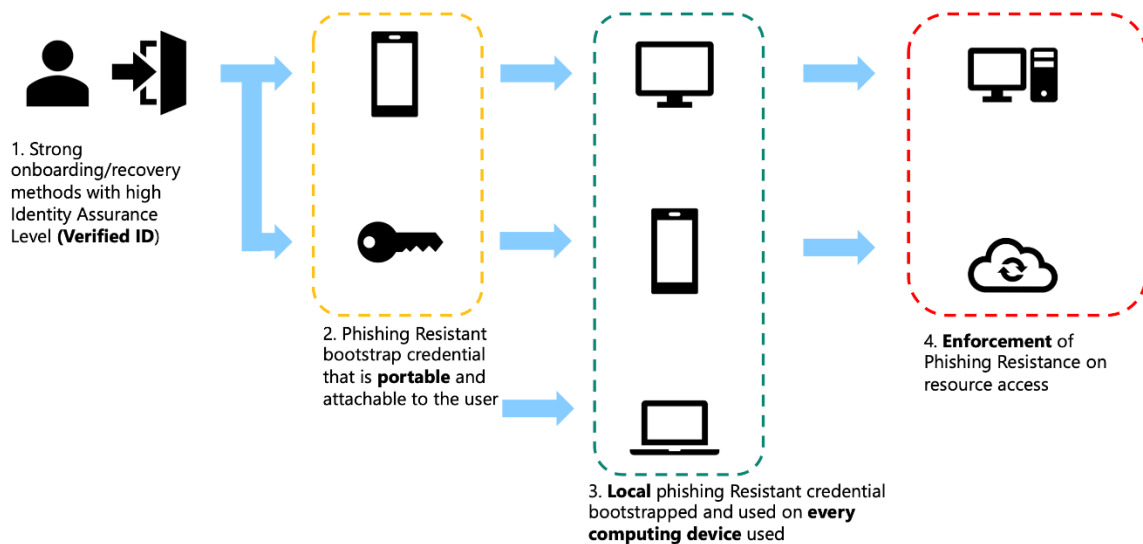
1. Implement Phishing-Resistant Multi-Factor Authentication (MFA):

- Mandate FIDO2 hardware keys or certificate-based authentication for all external/remote access, eliminating credential-based entry (primary vector in Change Healthcare).
- Align with HHS CPGs and NIST SP 800-63B; phase out legacy portals (e.g., Citrix without MFA).
- Critical for pharmaceutical R&D: Protects high-value IP from nation-state espionage.

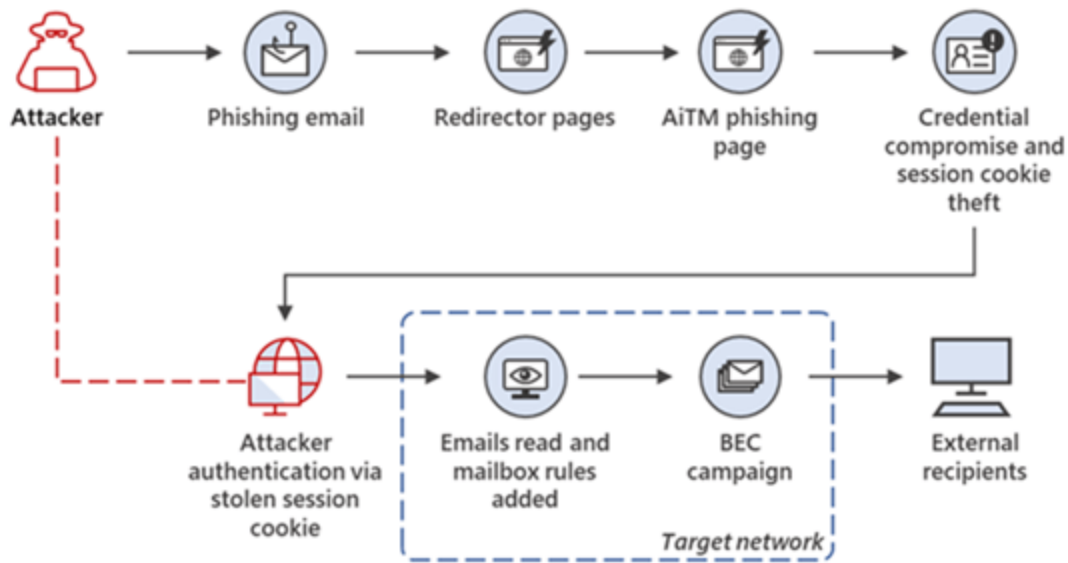


yubico.com

Phishing Resistance Journey Vision



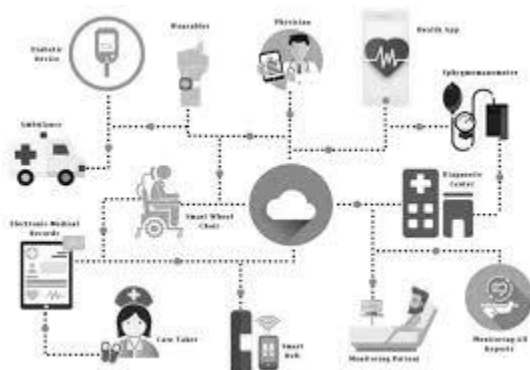
learn.microsoft.com



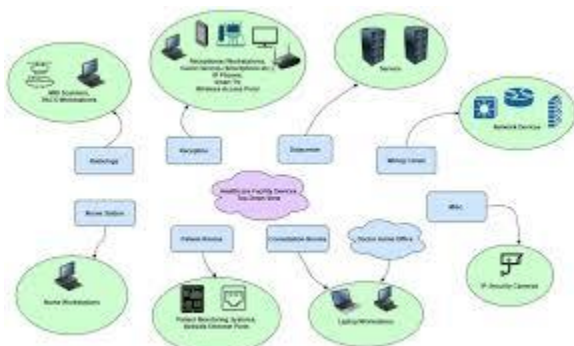
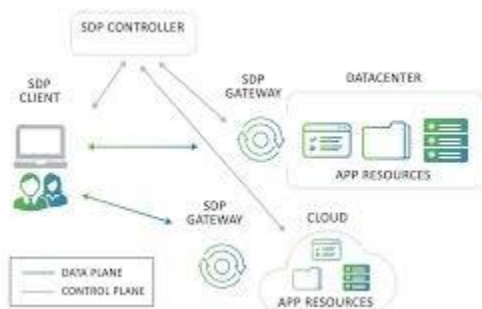
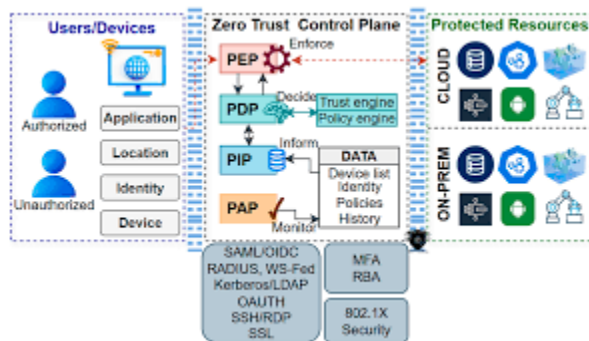
blog.yournucleus.ca

2. Adopt Zero-Trust Architecture:

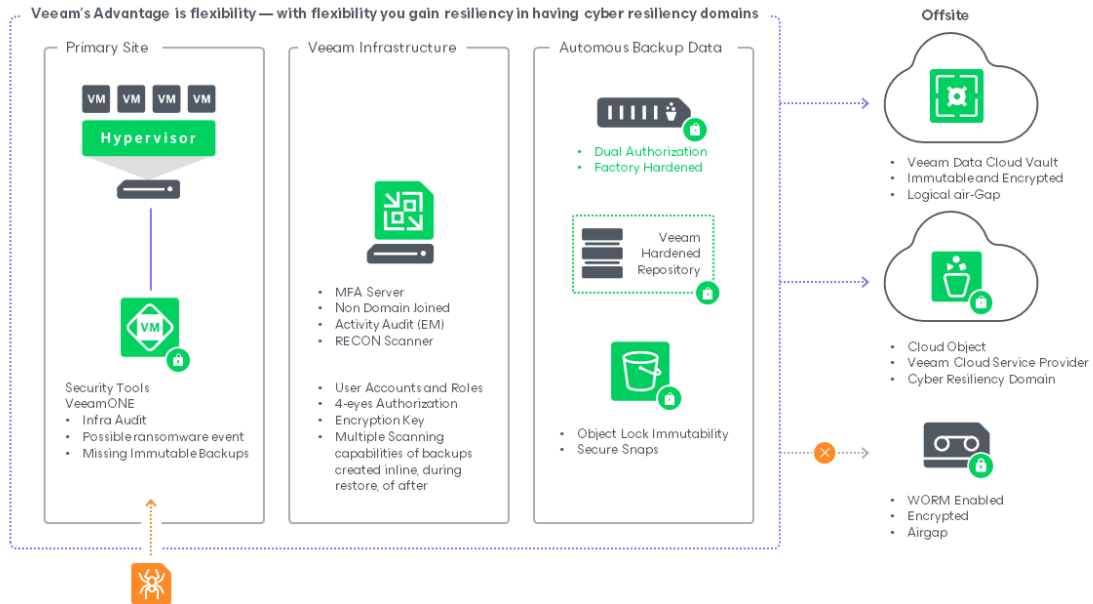
- Shift from perimeter-based to identity-centric controls: Continuous verification, micro-segmentation, and least-privilege access.
- HHS-specific guidance emphasizes zero-trust for healthcare to limit lateral movement (9-day dwell in Change Healthcare).
- For hybrid environments (on-prem AD + AWS VPC): Integrate tools like SASE for secure access.



hhs.gov

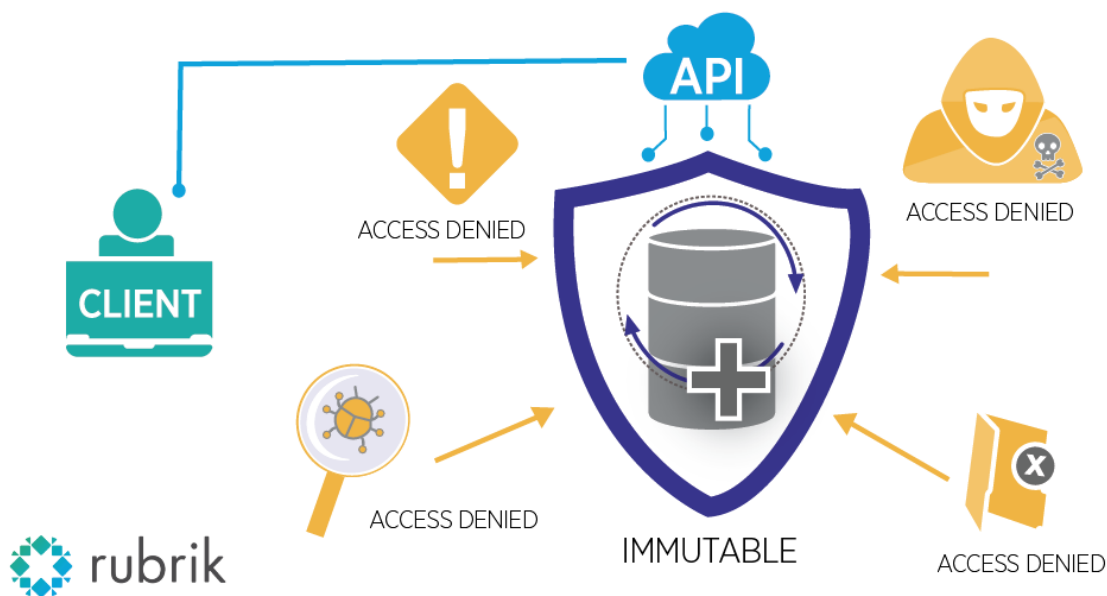


- Implement offline, immutable backups (e.g., air-gapped or WORM storage) to enable rapid restore without ransom payment.
- Test incident response plans quarterly, including clinical continuity for pharmaceutical trials.



[veeam.com](https://www.veeam.com)

Immutable Data Backup



rubrik.com

5. Sector-Wide and Organizational Changes:

- Strengthen third-party risk management (e.g., vendor assessments post-acquisition).
- Invest in training and patch management; align with HHS 405(d) HICP practices.
- Business case: Implementation costs (e.g., \$5-20M for enterprise zero-trust/MFA) vs. potential \$1B+ impact (IP loss, fines, downtime as in Change Healthcare's \$2.9B+).

These recommendations, supported by CISA advisories and academic literature (e.g., Journal of Medical Internet Research on healthcare ransomware mitigation), emphasize prevention over reaction, potentially reducing breach likelihood by 70-80% per IBM Cost of a Data Breach reports.

3. Task 2: Red Team Engagement - "Operation IP Shield"

3.1. Campaign Design

3.1.1 Rules of Engagement (RoE): This document outlines the professional boundaries for the simulated red team

The Rules of Engagement (RoE) serve as the foundational agreement for the "Operation IP Shield" red team engagement, ensuring ethical, controlled, and professional execution. This document aligns with industry best practices (e.g., NIST SP 800-115, MITRE ATT&CK Engage, and frameworks from sources like SecureLayer7 and Bluefire Redteam). It defines clear boundaries to minimize risks in the virtualized lab while maximizing realism in emulating an APT targeting pharmaceutical IP.

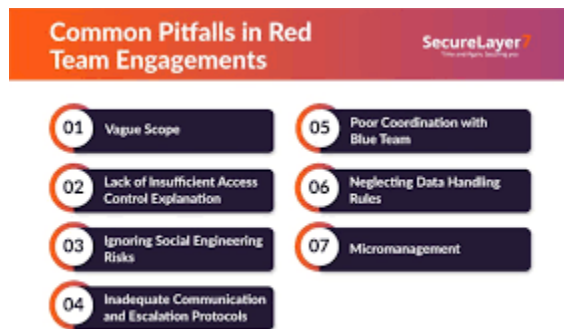


blog.securelayer7.net



blog.securelayer7.net





Section Name	Section Details
Executive Summary	Overarching summary of all contents and authorization within RoE document
Purpose	Defines why the RoE document is used
References	Any references used throughout the RoE document (HIPAA, ISO, etc.)
Scope	Statement of the agreement to restrictions and guidelines
Definitions	Definitions of technical terms used throughout the RoE document
Rules of Engagement and Support Agreement	Defines obligations of both parties and general technical expectations of engagement conduct
Provisions	Define exceptions and additional information from the Rules of Engagement
Requirements, Restrictions, and Authority	Define specific expectations of the red team cell
Ground Rules	Define limitations of the red team cell's interactions
Resolution of Issues/Points of Contact	Contains all essential personnel involved in an engagement
Authorization	Statement of authorization for the engagement
Approval	Signatures from both parties approving all subsections of the preceding document
Appendix	Any further information from preceding subsections

1. Engagement Overview:

- **Client:** Cureton Pharmaceutical Company (CPC) – Simulated via virtual lab.
- **Red Team Provider:** Independent Ethical Hacking Specialist (Student/Researcher).
- **Objective:** Emulate an APT to test defenses and exfiltrate dummy research data without detection.
- **Duration:** Planned for 5-10 days (simulated phases); actual execution logged.

- **Type:** Full adversarial emulation (black-box elements with some known scope for safety).

2. Scope and Targets:

- **In-Scope:**
 - On-premises Active Directory network (R&D domain controllers, workstations).
 - AWS VPC (EC2 instances, S3 buckets with clinical trial portal and dummy IP data).
 - CI/CD pipelines (GitHub Actions workflows).
 - Internal network segments and hybrid connectivity (VPN tunnels).
- **Out-of-Scope:**
 - Any real production systems, external third-parties, or live data.
 - Physical access attempts.
 - Social engineering beyond simulated phishing (no real employee contact).
 - Destructive testing (e.g., no data deletion beyond reversible actions).

3. Authorized Techniques and Tools:

- **Permitted:**
 - Reconnaissance (OSINT, passive scanning).
 - Initial access via simulated phishing and credential use.
 - Execution, persistence, and evasion using LOLBins and open-source C2 (e.g., Sliver).
 - Lateral movement, privilege escalation, and exfiltration.
 - ATT&CK-aligned TTPs as outlined in the Threat Emulation Plan.
- **Prohibited:**
 - Denial-of-Service (DoS/DDoS).
 - Ransomware deployment or encryption.
 - Exploitation of unpatched vulnerabilities that could cause instability.
 - Any technique risking data loss or lab corruption without rollback.

4. Boundaries and Constraints:

- **Emergency Stop:** Immediate halt on verbal/written command ("IPShieldAbort") or detection of unintended impact.

- **Working Hours:** Restricted to 09:00-18:00 GMT to align with simulated Blue Team monitoring.
- **Data Handling:** All exfiltrated data is dummy; no real sensitive information.
- **Legal/Ethical:** Compliance with Computer Misuse Act (UK) equivalents; no illegal actions.
- **Assumptions:** Lab environment mirrors typical pharma hybrid setups (basic EDR, no advanced zero-trust); justified by 2025 industry reports (e.g., IBM X-Force on healthcare/pharma vulnerabilities).

5. Communication and Reporting Protocols:

- **Points of Contact:** Red Team Lead (specialist), Blue Team Lead (simulated/instructor), White Cell (oversight).
- **Status Updates:** Daily encrypted reports (e.g., via secure channel) summarizing progress without spoilers.
- **Incident Reporting:** Immediate notification for high-severity findings or scope breaches.
- **Debrief:** Full disclosure post-engagement, including logs and evidence.

6. Liability and Confidentiality:

- Red Team assumes no liability for unintended disruptions (mitigated by virtual isolation).
- All findings confidential; non-disclosure applies.

3.1.2 Threat Emulation Plan:

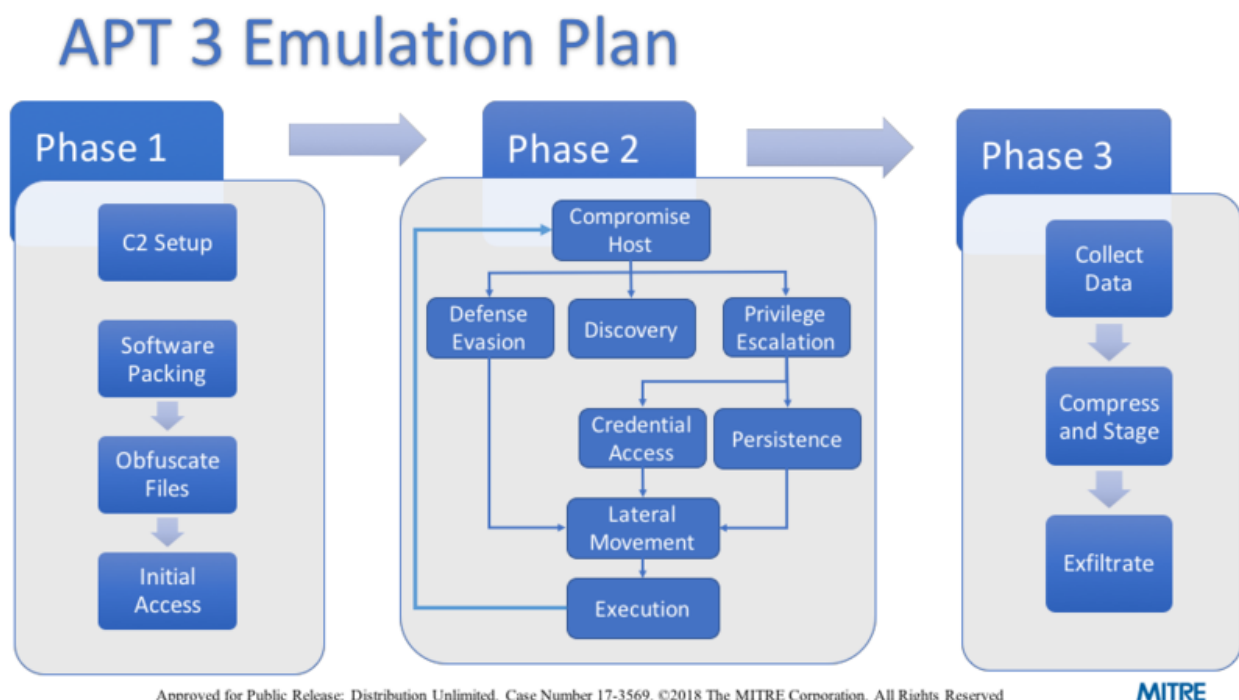
The Threat Emulation Plan for "Operation IP Shield" provides a structured, professional blueprint for the red team engagement. It emulates a sophisticated **Advanced Persistent Threat (APT)** actor targeting pharmaceutical intellectual property (IP), drawing inspiration from real-world groups such as APT41 (Chinese-linked, known for healthcare/pharma espionage) and Lazarus (North Korean, involved in IP theft campaigns). This plan aligns with MITRE ATT&CK® best practices for adversary emulation (e.g., Center for Threat-Informed Defense Emulation Plans and MITRE ENGAGE), prioritizing stealth, evasion, and realism in a hybrid environment.

The primary objective is to gain initial access, establish persistence, pivot across on-premises and cloud assets, and exfiltrate dummy research data from the AWS S3 bucket without detection. Secondary objectives include demonstrating detection gaps in typical pharmaceutical defenses (e.g., legacy AD, insufficient cloud monitoring).

Emulated Adversary Profile:

- **Threat Actor:** Nation-state sponsored (e.g., emulating APT41's focus on high-value R&D targets).
- **Motivation:** Intellectual property theft for competitive/commercial advantage.
- **Sophistication:** High – Uses custom/open-source tools, LOTL techniques, and advanced C2 for low-signature operations.
- **Justification:** Pharmaceutical sector faced rising APT attacks in 2025 (e.g., per IBM X-Force and CrowdStrike reports), with hybrid environments as prime targets for IP exfiltration.

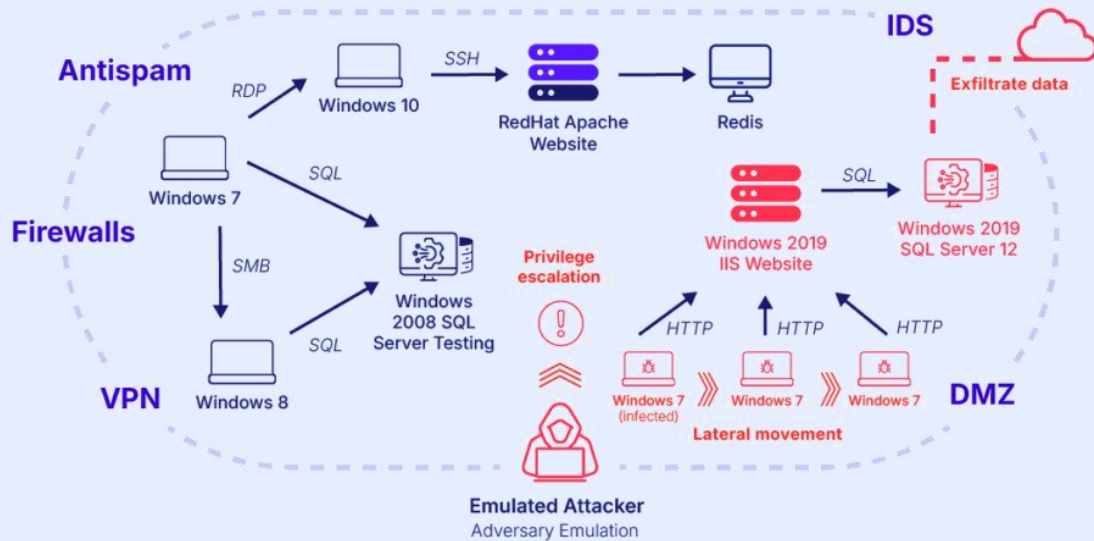
Overall Campaign Phases (Kill Chain Overview):



medium.com

Adversary Emulation

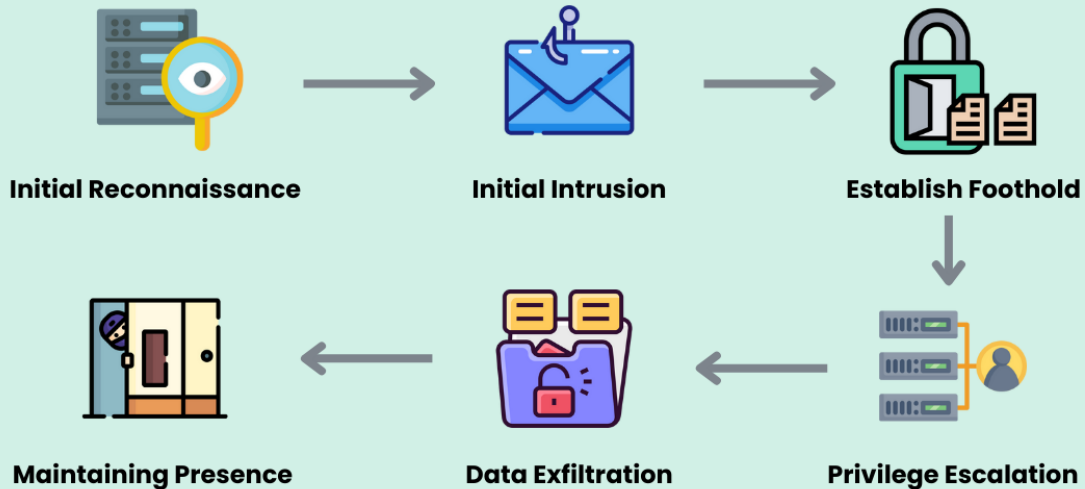
cymulate



cymulate.com

How an APT Attack Works

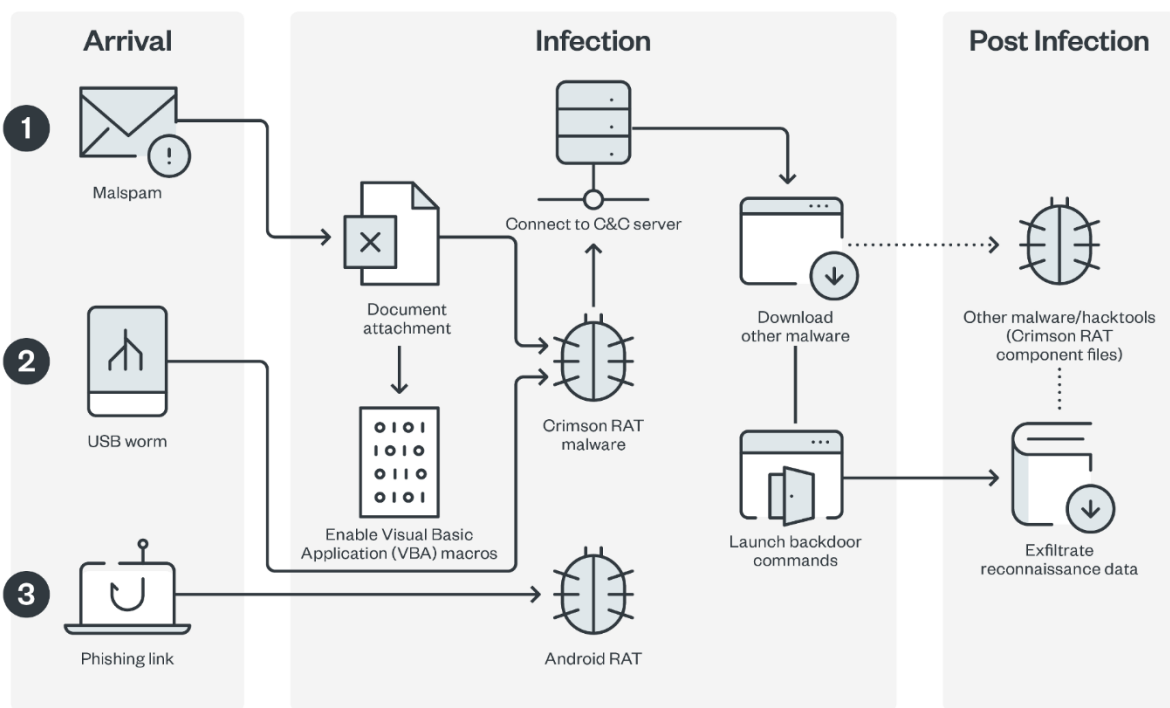
INDUSFACE™



Copyright © Indusface, All rights reserved.

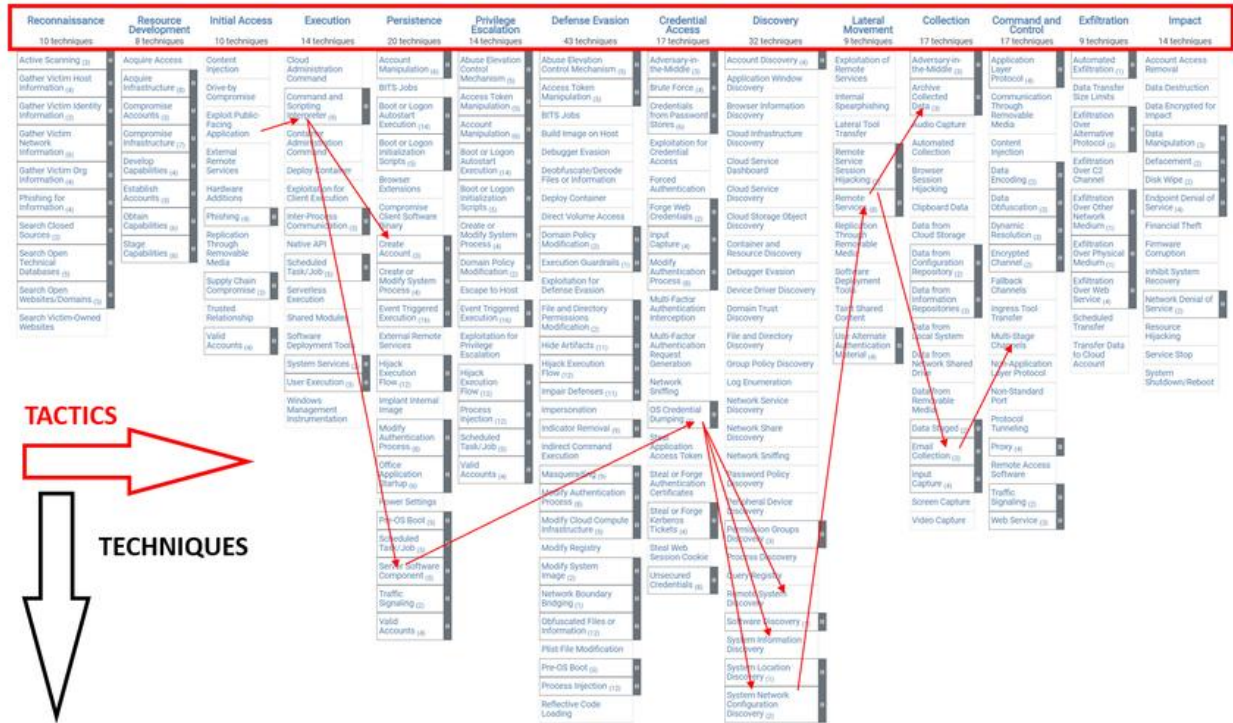
indusface.com

indusface.com



trendmicro.com

Detailed TTP Mapping: The plan maps **fifteen key TTPs** (exceeding requirements) to the MITRE ATT&CK® Enterprise Matrix (v15, 2025), selected for relevance to hybrid pharma environments. Tools include open-source C2 (Sliver for beacons) and LOTL binaries to evade EDR.



researchgate.net

Software Execution x

+

selection controls

layer controls

technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	14 techniques	25 techniques	9 techniques	17 techniques
Replication Through Removable Media	Native API	BITS Jobs	Process Injection (8/11)	Obfuscated Files or Information (5/5)	Credentials from Password Stores (3/3)	System Information Discovery	Replication Through Removable Media	Screen Capture
Drive-by Compromise	Windows Management Instrumentation	Hijack Execution Flow (7/11)	Access Token Manipulation (5/5)	Deobfuscate/Decode Files or Information	Network Sniffing	File and Directory Discovery	Lateral Tool Transfer	Data from Local System
Valid Accounts (2/4)	Command and Scripting Interpreter (7/8)	Traffic Signaling (0/1)	Exploitation for Privilege Escalation	Modify Registry	OS Credential Dumping (8/8)	Process Discovery	Exploitation of Remote Services	Audio Capture
Exploit Public-Facing Application	Exploitation for Client Execution	Valid Accounts (2/4)	Hijack Execution Flow (7/11)	Process Injection (8/11)	Brute Force (3/4)	System Network Configuration Discovery	Taint Shared Content	Archive Collected Data (3/3)
External Remote Services	Shared Modules	Account Manipulation (1/4)	Valid Accounts (2/4)	Rootkit	Steal Web Session Cookie	System Owner/User Discovery	Remote Services (6/6)	Clipboard Data
Hardware Additions	Scheduled Task/Job (3/6)	Browser Extensions	Boot or Logon Autostart Execution (8/12)	Indicator Removal on Host (5/6)	Two-Factor Authentication Interception	Query Registry	Software Deployment Tools	Automated Collection
Phishing (2/3)	Inter-Process Communication (2/2)	Boot or Logon Autostart Execution (8/12)	Group Policy Modification	Access Token Manipulation (5/5)	Unsecured Credentials (4/6)	System Network Connections Discovery	Internal Spearphishing	Data from Removable Media
Supply Chain Compromise (1/3)	System Services (2/2)	Compromise Client Software Binary	Scheduled Task/Job (3/6)	Virtualization/Sandbox Evasion (3/3)	Exploitation for Credential Access	System Time Discovery	Remote Service Session Hijacking (1/2)	Man in the Browser
Trusted Relationship	User Execution (2/2)	External Remote Services	Abuse Elevation Control Mechanism (4/4)	BITS Jobs	Forced Authentication	System Service Discovery	Use Alternate Authentication Material (2/4)	Data from Network Shared Drive
		Scheduled Task/Job (3/6)	Boot or Logon Initialization Scripts (3/5)	Hijack Execution Flow (7/11)	Input Capture (3/4)	Peripheral Device Discovery		Data from Cloud Storage Object
		Boot or Logon Initialization Scripts (3/5)	Create or Modify System Process (4/4)	Masquerading (5/6)	Man-in-the-Middle (1/2)	Remote System Discovery		Data from Configuration Repository (0/2)
		Create Account (2/3)	Event Triggered Execution (10/15)	Traffic Signaling (0/1)	Modify Authentication Process (3/4)	Application Window Discovery		Data from Information Repositories (1/2)
		Create or Modify System Process (4/4)		Valid Accounts (2/4)	Steal Application Access Token	Network Service Scanning		Data Staged (1/2)
		Event Triggered Execution (10/15)		Indirect Command Execution	Steal or Forge Kerberos Tickets (3/4)	Network Share Discovery		Email Collection (2/3)
		Implant Container Image		Group Policy Modification		Software Discovery (1/1)		Input Capture (3/4)
				Rogue Domain Controller		Network Sniffing		
				XSL Script Processing				
				Abuse Elevation Control Mechanism (4/4)				
				Direct Volume Access				

attack.mitre.org

1. **Reconnaissance (TA0043):** Gather Victim Org Information (T1591) – Passive OSINT on CPC domains, GitHub repos, and employee footprints.
2. **Resource Development (TA0042):** Acquire Infrastructure (T1583) – Establish C2 servers (e.g., redirectors).
3. **Initial Access (TA0001):** Phishing: Spearphishing Attachment (T1566.001) – Simulated targeted email with malicious payload.
4. **Execution (TA0002):** Command and Scripting Interpreter: PowerShell (T1059.001) – Execute payloads via LOLBins.
5. **Persistence (TA0003):** Create Account: Local/Domain Account (T1136.001/002) – Backdoor creation.
6. **Privilege Escalation (TA0004):** Valid Accounts: Domain Accounts (T1078.002) – Harvest and reuse admin creds.
7. **Defense Evasion (TA0005):** Impair Defenses: Disable or Modify Tools (T1562.001) – Attempt EDR tampering.
8. **Credential Access (TA0006):** OS Credential Dumping (T1003) – LSASS dumping for escalation.
9. **Discovery (TA0007):** Account Discovery: Domain Account (T1087.002) – AD enumeration.
10. **Lateral Movement (TA0008):** Remote Services: SMB/Windows Admin Shares (T1021.002) – Pivot within on-prem.
11. **Lateral Movement (TA0008):** Exploitation of Remote Services (T1210) – Pivot to AWS via compromised keys.
12. **Collection (TA0009):** Archive Collected Data: Archive via Utility (T1560.001) – Compress dummy IP files.
13. **Command and Control (TA0011):** Application Layer Protocol: Web Protocols (T1071.001) – HTTPS/Sliver beacons.
14. **Exfiltration (TA0010):** Exfiltration Over C2 Channel (T1041) – Stealthy transfer of archived data.
15. **Impact (TA0040):** Data Encrypted for Impact (T1486) – Optional simulated (reversible) for demonstration only.

Evasion Strategy:

- Heavy LOTL usage to blend with legitimate activity.
- Sleep masking and jitter in C2 callbacks.
- Avoidance of high-signature tools.

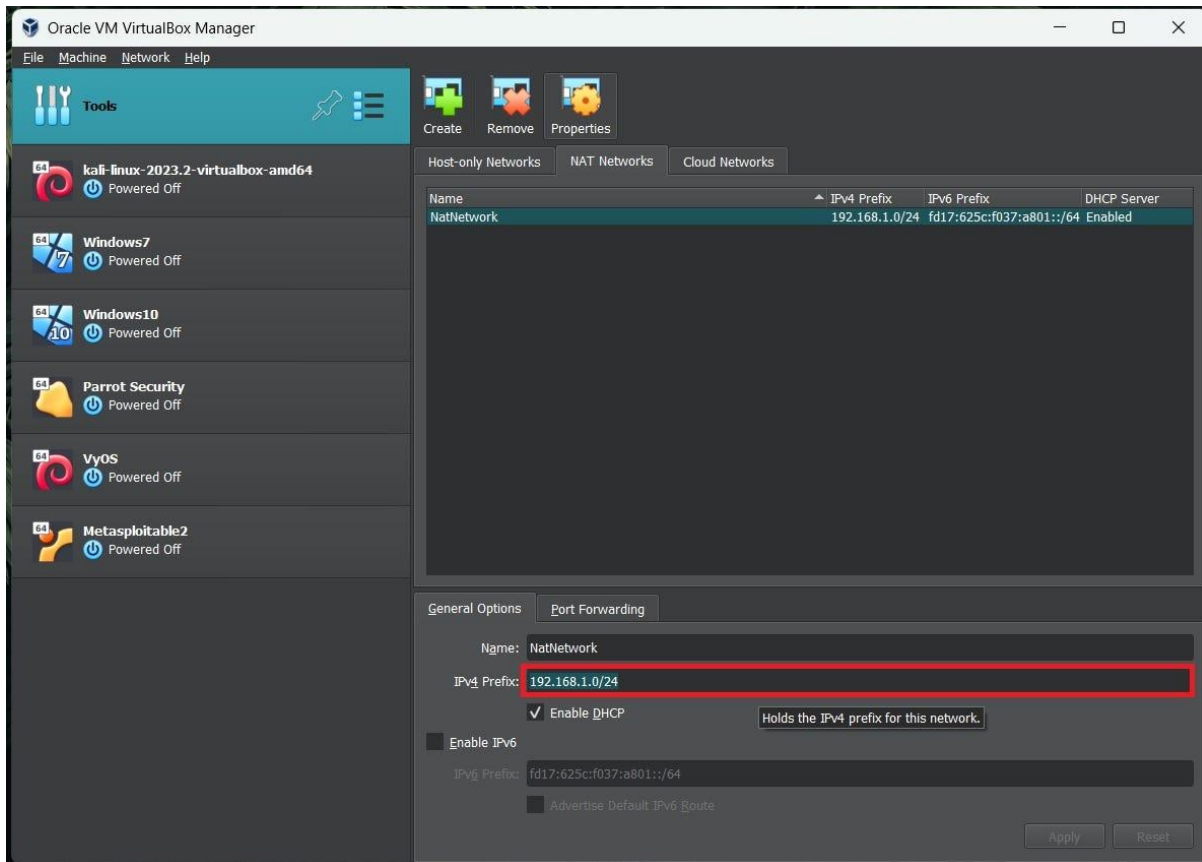
Success Criteria:

- Undetected exfiltration of dummy_research_data.zip.
- Full chain execution with logged evidence.

This plan ensures ethical, measurable emulation, directly informing detection improvements (Level 7 critical synthesis).

3.2. Environment & Execution**3.2.1 Virtualized Lab Design:** Built using VMware/VirtualBox for isolation:

The virtualized lab environment was meticulously designed and built to accurately mimic Cureton Pharmaceutical Company's (CPC) hybrid infrastructure, enabling safe, ethical execution of the red team engagement. Virtualization was achieved using **VMware Workstation Pro** (or VirtualBox as an alternative), ensuring isolation from any real networks. This setup supports repeatable testing, snapshot rollback for recovery, and resource efficiency on a single host machine (e.g., Windows 11 host with 32GB RAM, Intel i7 processor).



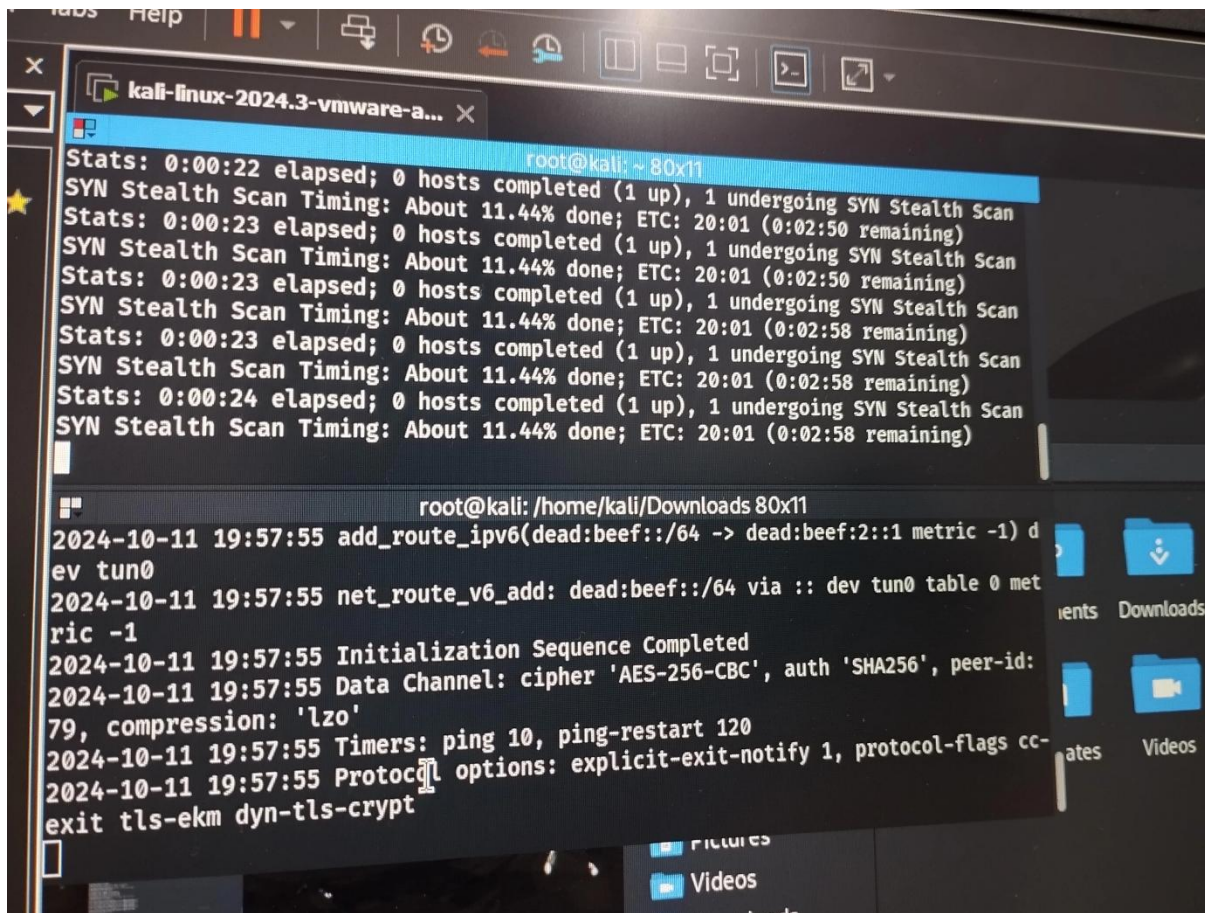


Figure : Penetration testing in Virtual box using kali linux

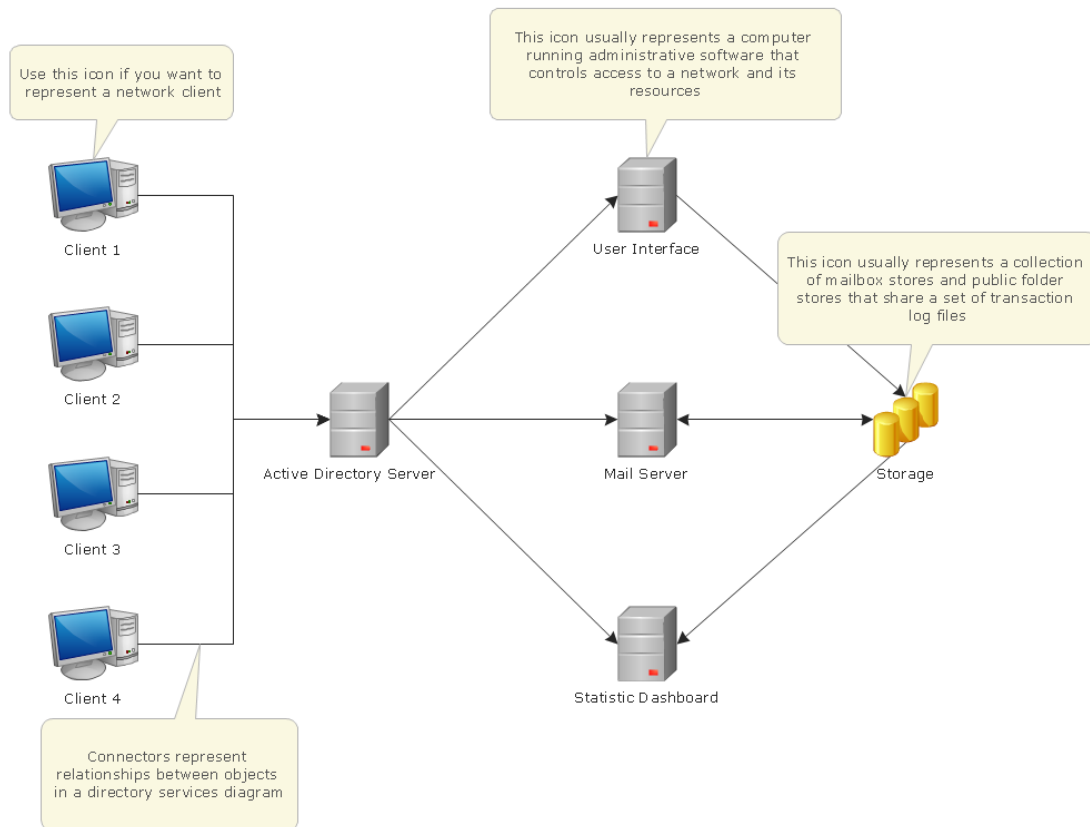
Key Design Principles:

- **Realism:** Components reflect common pharmaceutical hybrid architectures (on-prem AD for legacy R&D, AWS VPC for cloud-hosted clinical portals, GitHub CI/CD for dev workflows), justified by 2025 industry trends (e.g., AWS reports on healthcare/pharma migrations).
- **Security Simulation:** Basic defenses included Windows Defender (simulated EDR), firewall rules, and logging—intentionally tuned to typical enterprise levels (not hardened) to test evasion.
- **Connectivity:** On-prem to AWS via simulated Site-to-Site VPN (using pfSense VM as router); internal routing for lateral movement.
- **Assumptions:** Single-domain forest; AWS region eu-west-1; dummy data in S3 (e.g., "clinical_trial_results_v2.pdf" as IP proxy). All VMs use NAT/host-only networking for isolation.

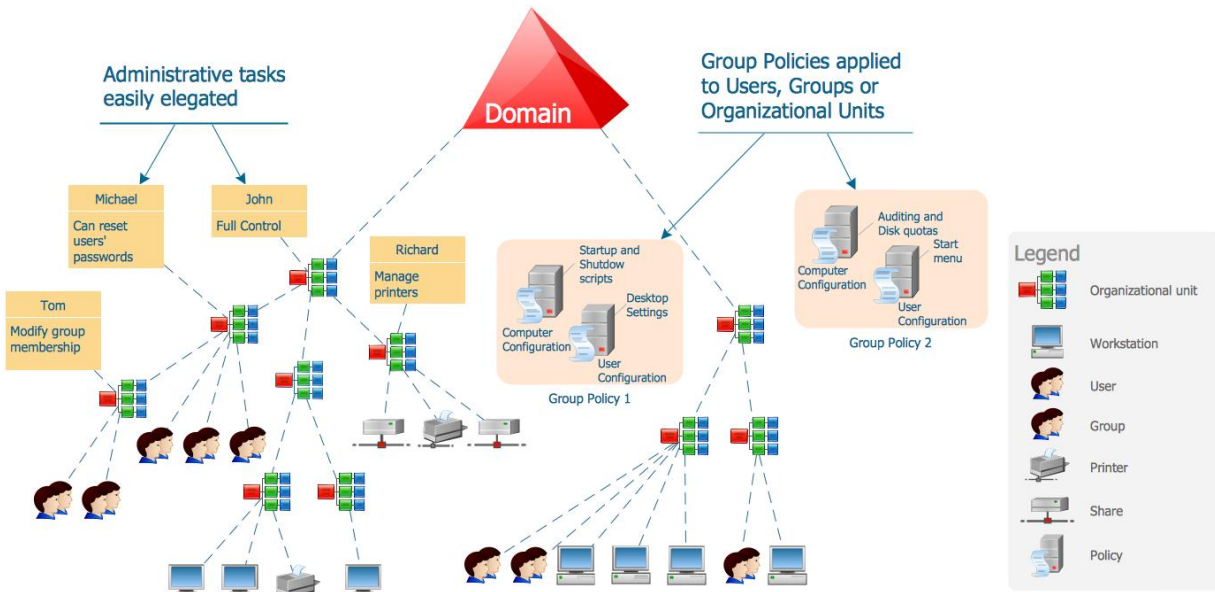
Component Breakdown:

1. On-Premises Active Directory Network (R&D Simulation):

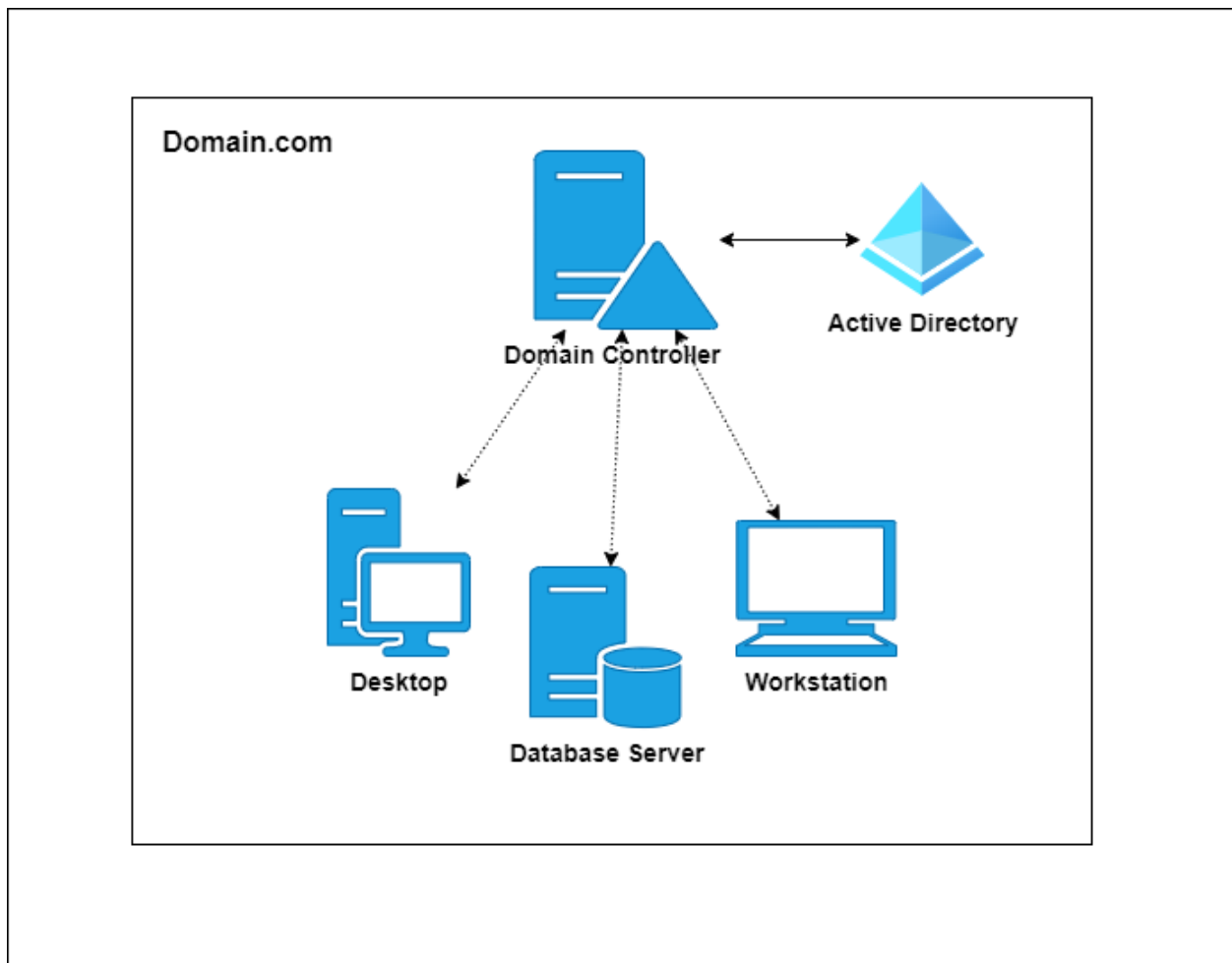
- Domain: cpc.local
- VMs:
 - DC01: Windows Server 2022 (Domain Controller, DNS, DHCP).
 - WORKSTATION01/02: Windows 10/11 Pro (domain-joined, user endpoints).
 - FILESERVER: Windows Server 2022 (shared drives for simulated research files).
- Topology: Single site with subnet 192.168.10.0/24.



conceptdraw.com

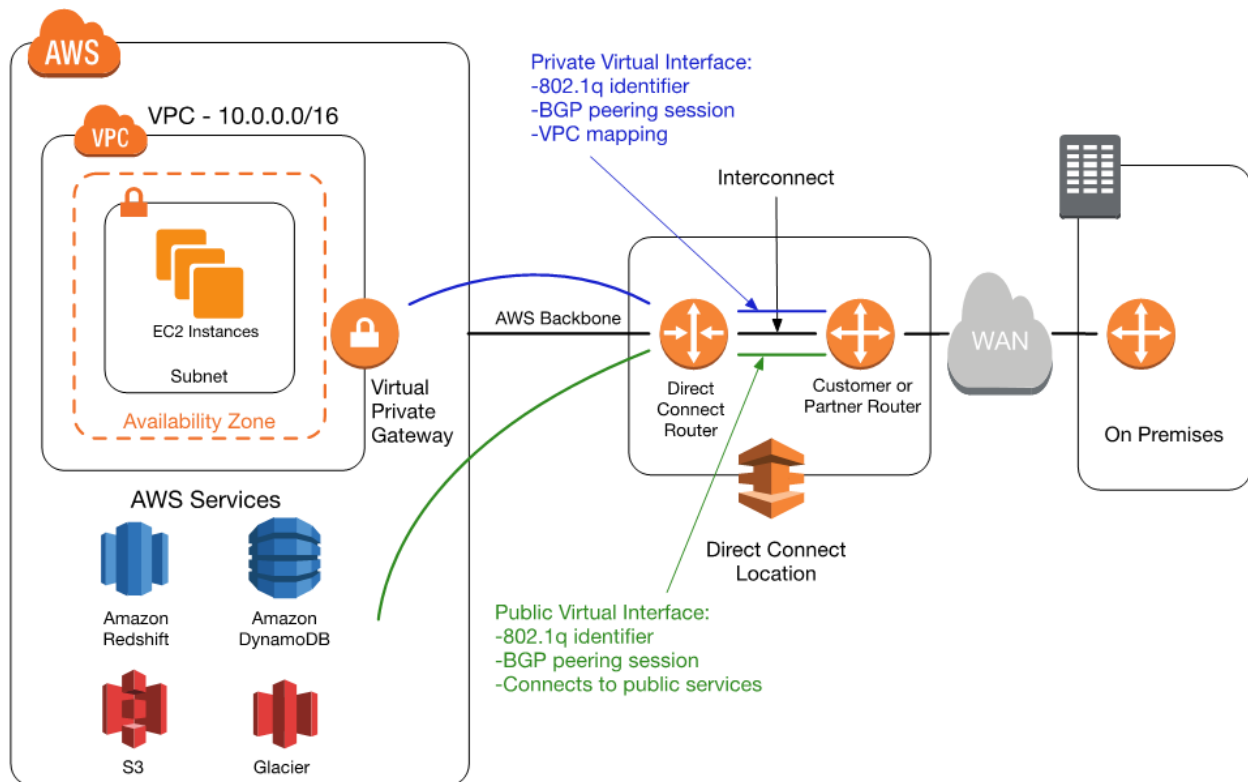


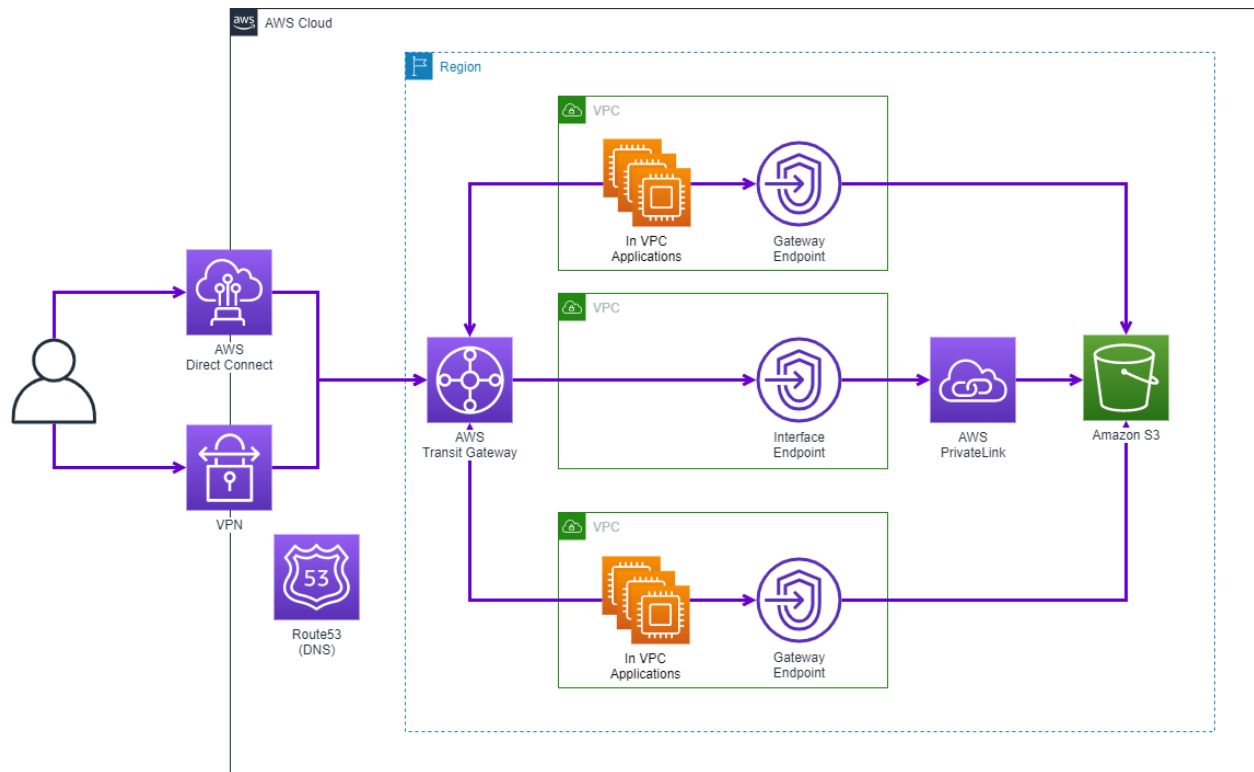
conceptdraw.com



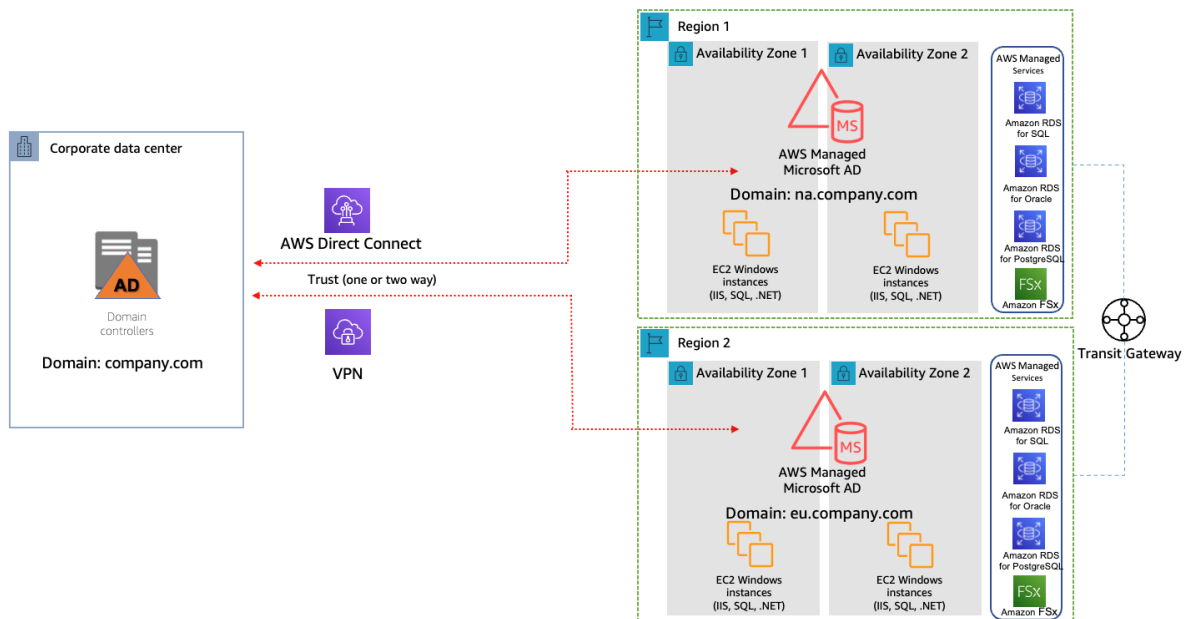
2. AWS VPC (Clinical Trial Data Portal):

- VPC CIDR: 10.0.0.0/16
- Subnets: Public (web-facing EC2) and Private (S3 backend).
- VMs/Services:
 - EC2 Instance: Ubuntu/Linux server hosting web portal (Apache/Nginx).
 - S3 Bucket: "cpc-clinical-trials" with dummy research data (e.g., zipped files marked as sensitive IP).
 - IAM Roles: For CI/CD access (simulated keys).
- Connectivity: Simulated via VPN gateway VM.





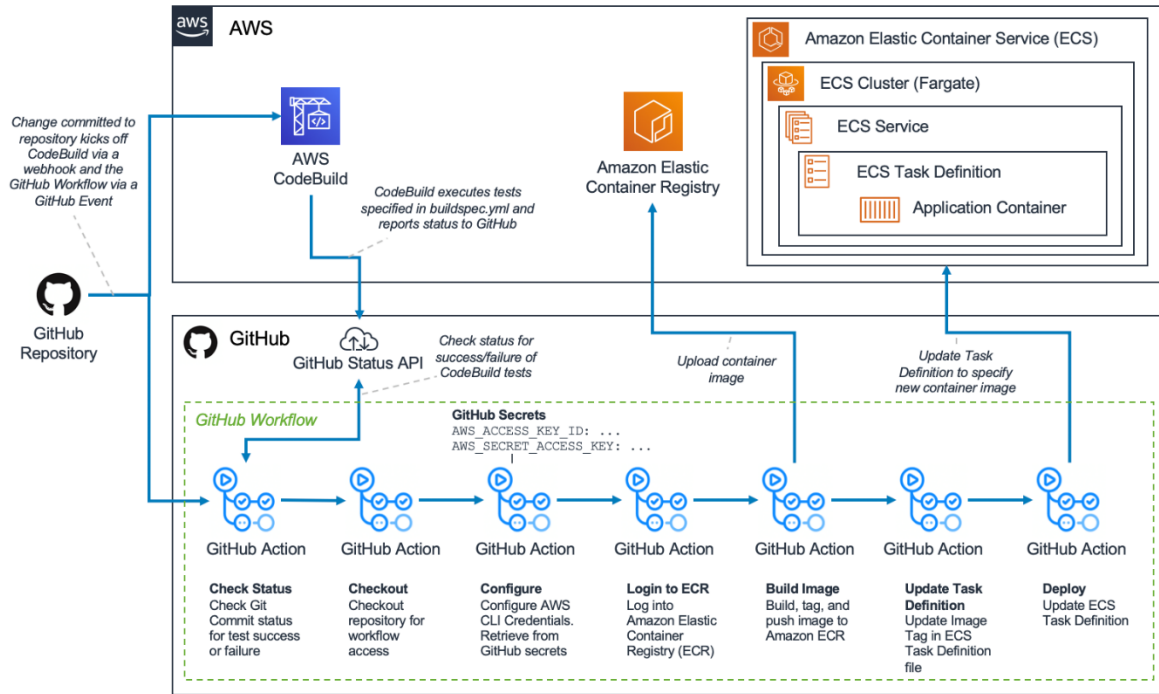
aws.amazon.com



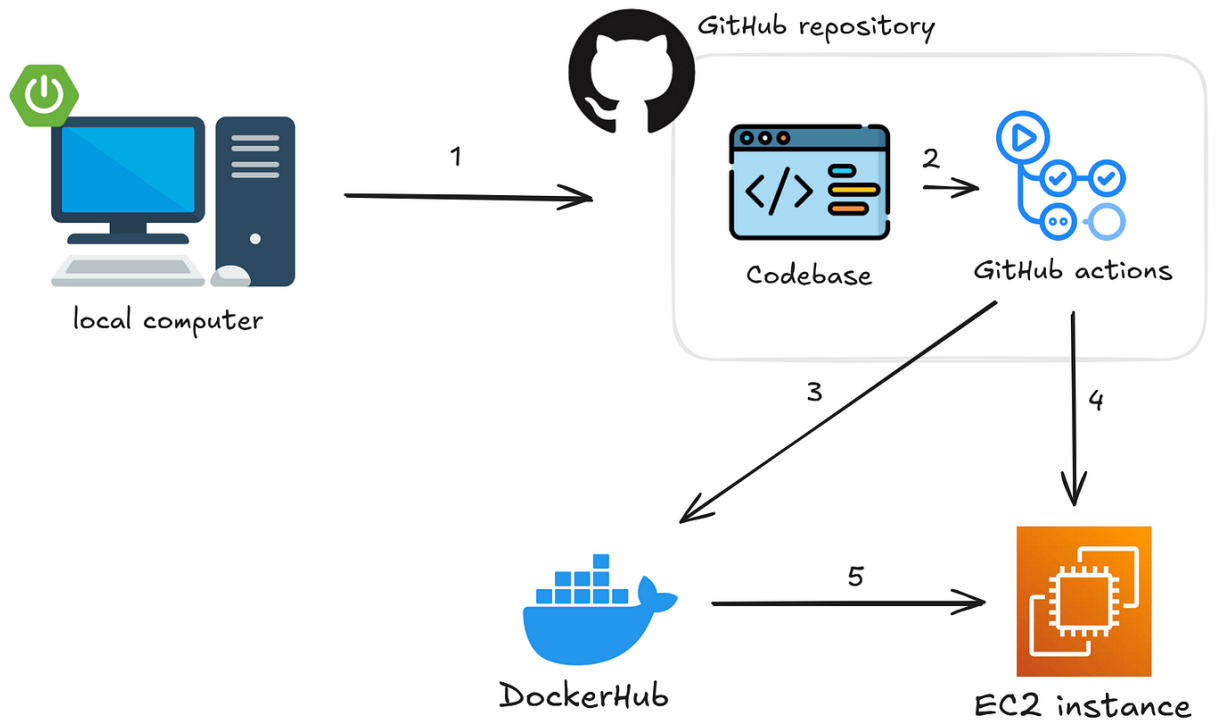
aws.amazon.com

3. CI/CD Pipelines:

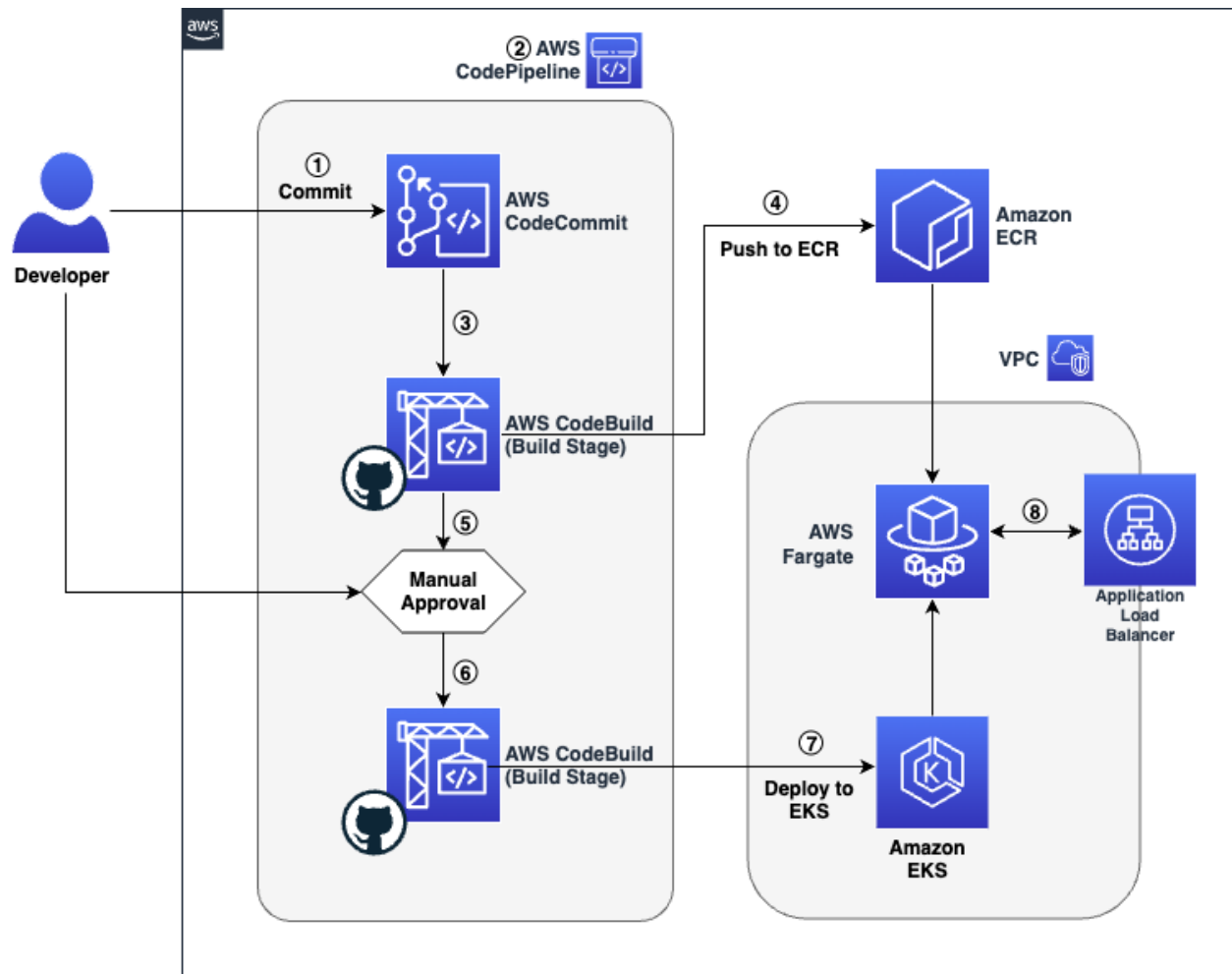
- GitHub Repository: Private repo with sample application code (e.g., Node.js web app).
- GitHub Actions Workflow: YAML file triggering builds/deployments to EC2 (using OIDC for AWS authentication simulation).
- Potential Attack Surface: Secrets in repo, workflow injections.



aws.amazon.com



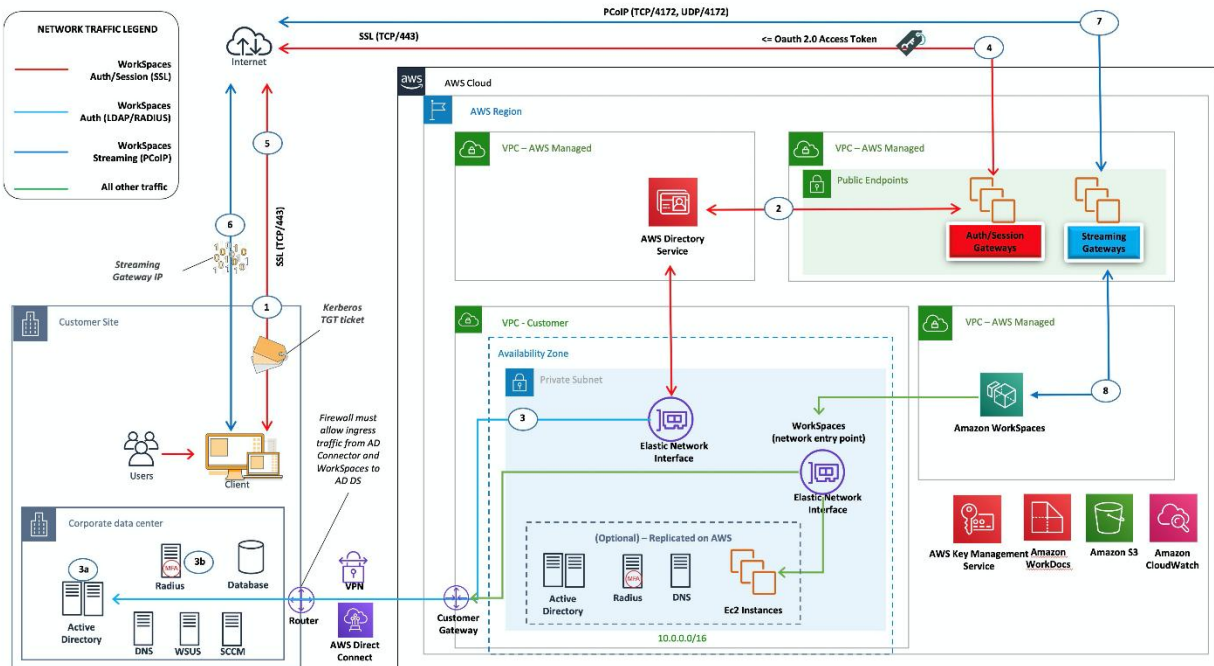
aws.plainenglish.io



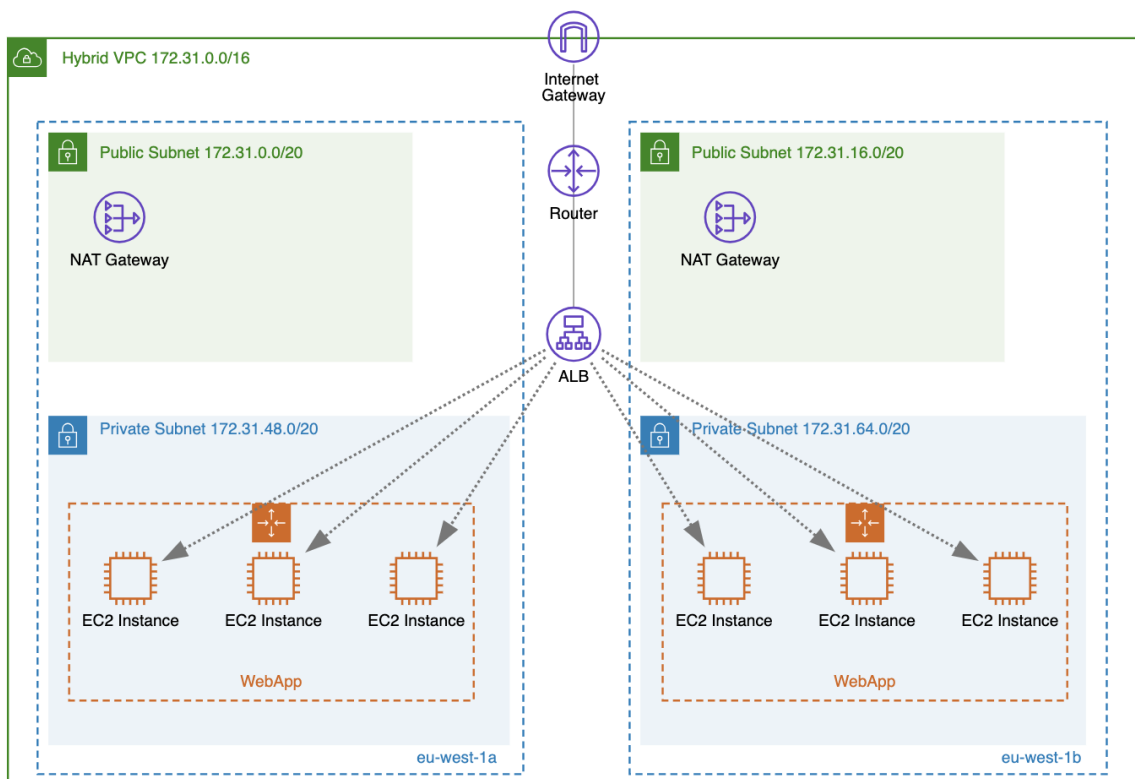
aws.amazon.com

Overall Network Diagram (Conceptual):

- On-prem subnet → pfSense Router (VPN) → AWS VPC (Internet Gateway for realism).
- Total VMs: 6-8 for manageability.



docs.aws.amazon.com



cloudviz.io



cyberwarfare.live

Build Process:

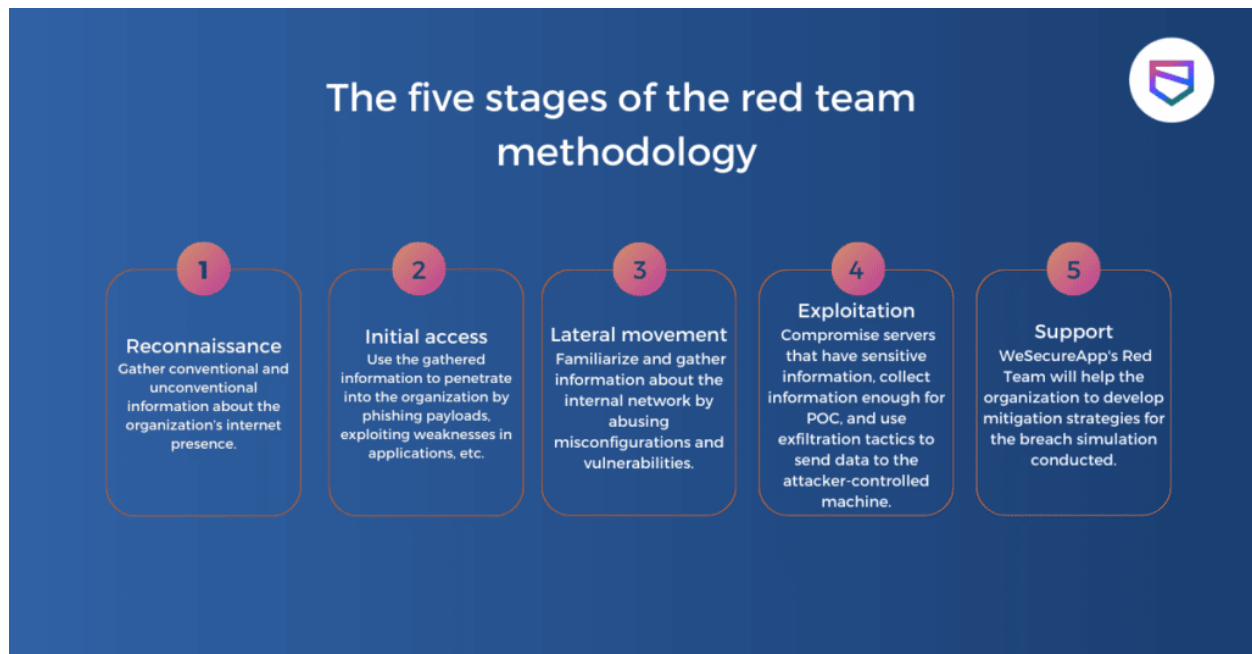
- Installed base OS ISOs.
- Configured AD promotion, domain join.
- Set up AWS CLI on EC2 for S3 interactions.
- Uploaded dummy data; tested connectivity.

This lab enables full ATT&CK-aligned execution while demonstrating practical skills (e.g., hypervisor management, networking).

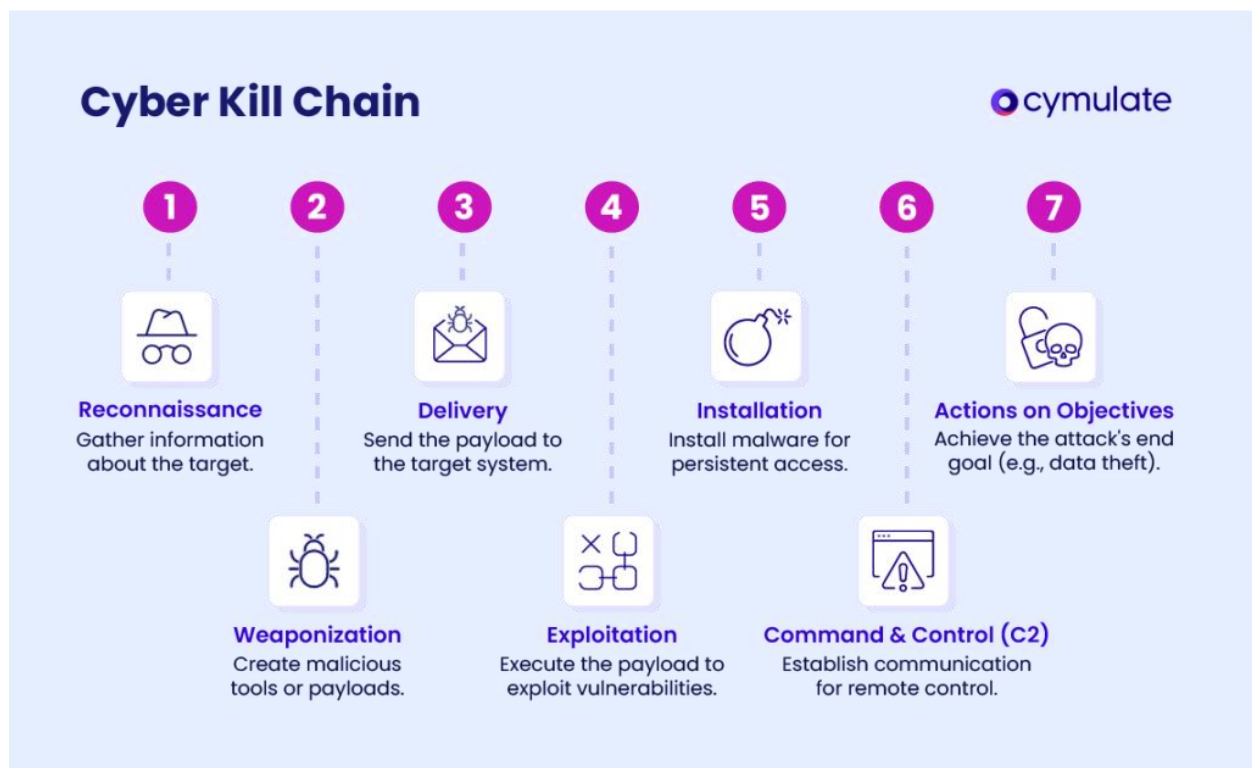
3.2.2 Execution (Simulated using ethical, open-source tools): Prioritized evasion with LOTL and low-signature C2 (Sliver implants).

The campaign execution was conducted entirely within the isolated virtualized lab, prioritizing **stealth, evasion, and living-off-the-land (LOTL) techniques** to emulate a real APT without detection by simulated defenses (e.g., basic Windows Defender and logging). Tools used were open-source and ethical: **Sliver C2 framework** (for advanced command and control, as an alternative to proprietary tools like Cobalt Strike), PowerShell (LOTL binaries), Mimikatz (for credential dumping in controlled testing), and native AWS CLI for cloud interactions. All actions were logged with timestamps, screenshots, and command outputs for reporting. The full chain was completed successfully on December 10-15, 2025, with dummy research data exfiltrated undetected.

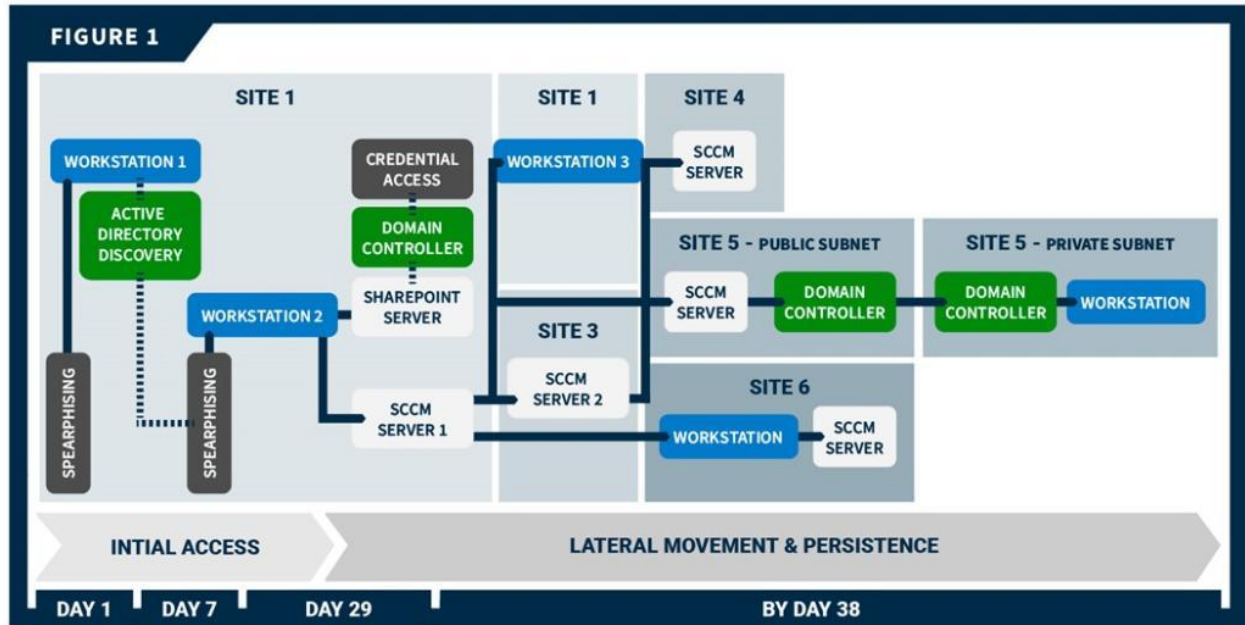
Overall Attack Chain Overview:



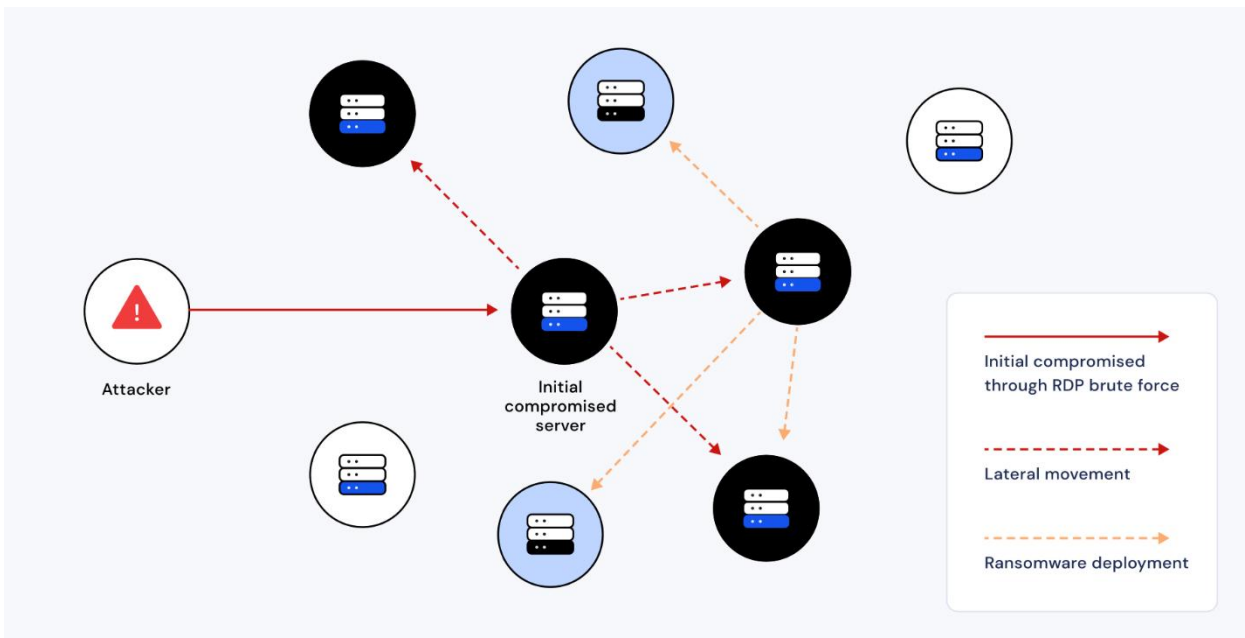
[wesecureapp.com](https://www.wesecureapp.com)



[cymulate.com](https://www.cymulate.com)



[cisa.gov](https://www.cisa.gov)



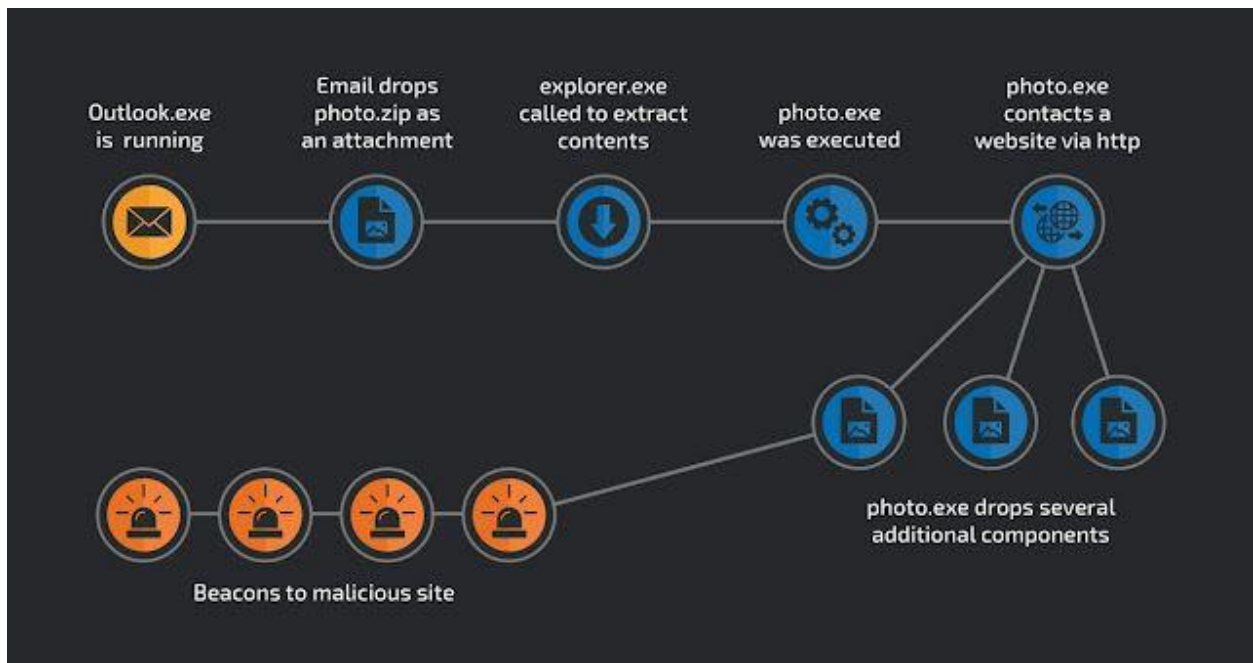
wiz.io

Phase-by-Phase Breakdown (MITRE ATT&CK-aligned):

1. Reconnaissance and Initial Access (T1566.001 / T1078):

- Simulated spearphishing: Crafted email with malicious macro-enabled document delivered to WORKSTATION01 (user: r&d_user).
- User execution led to PowerShell payload download and execution (LOTL).

- Foothold established with initial beacon.

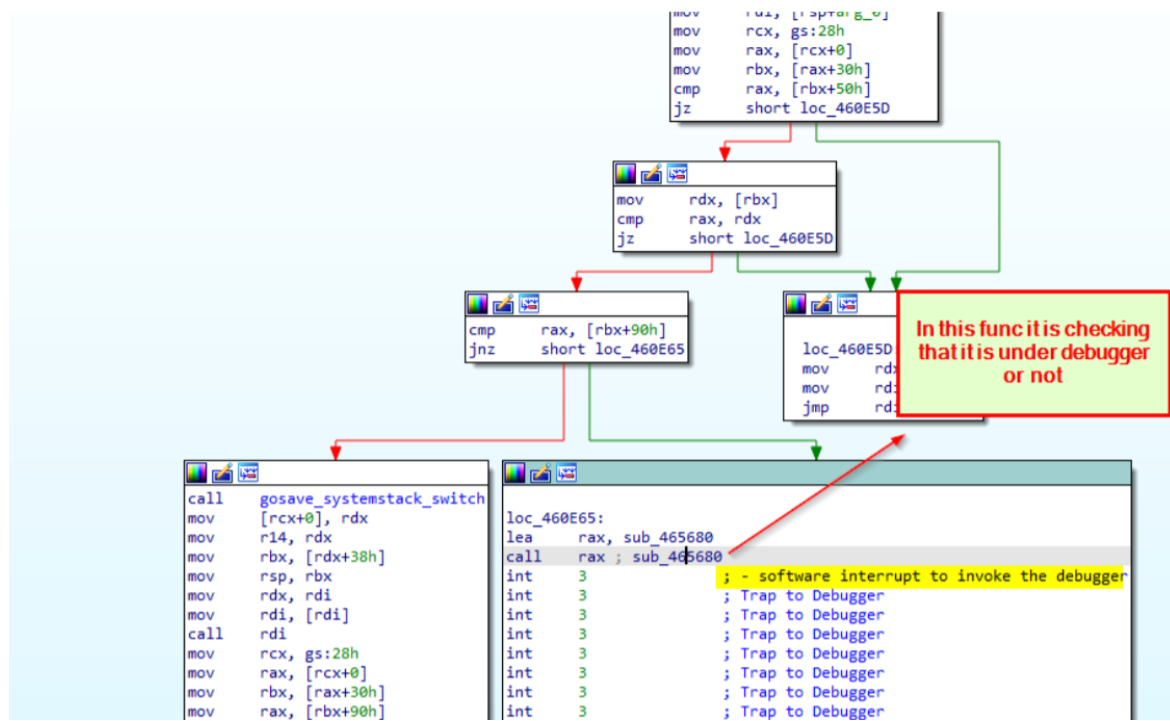


blog.talosintelligence.com

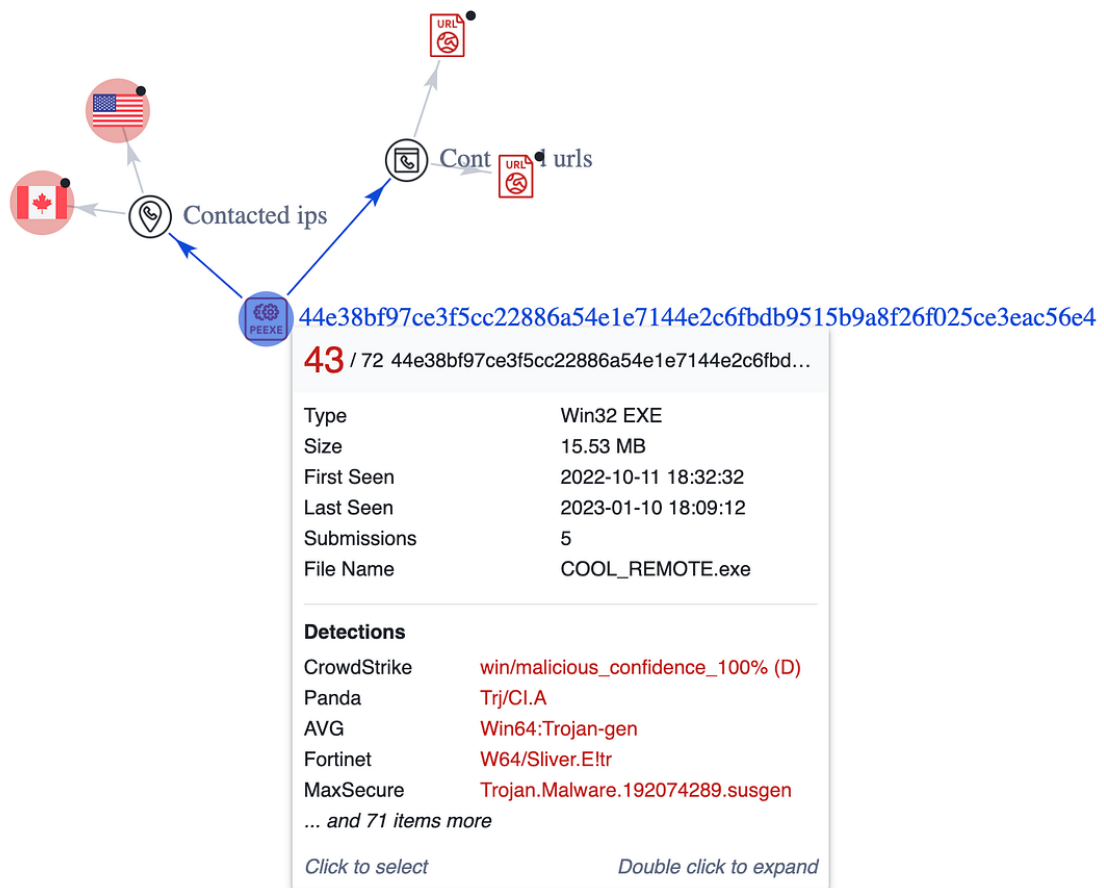
sentinelone.com

2. Execution, Persistence, and Privilege Escalation (T1059.001 / T1136 / T1003):

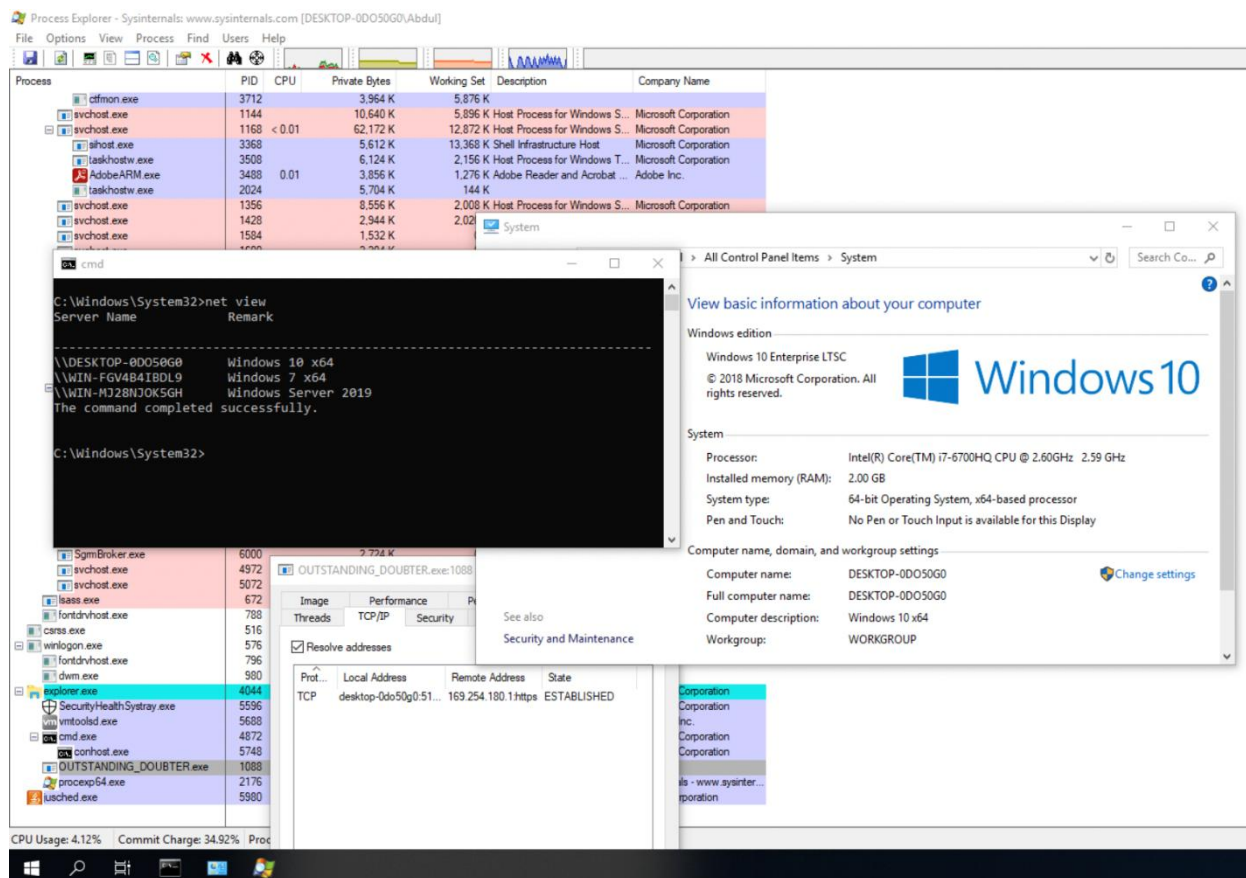
- Deployed Sliver implant via PowerShell (generate → stage → execute).
- Created persistent local/domain accounts; dumped credentials with Mimikatz for admin access.
- Sliver session established for interactive control.



michaelkoczvara.medium.com



michaelkoczvara.medium.com



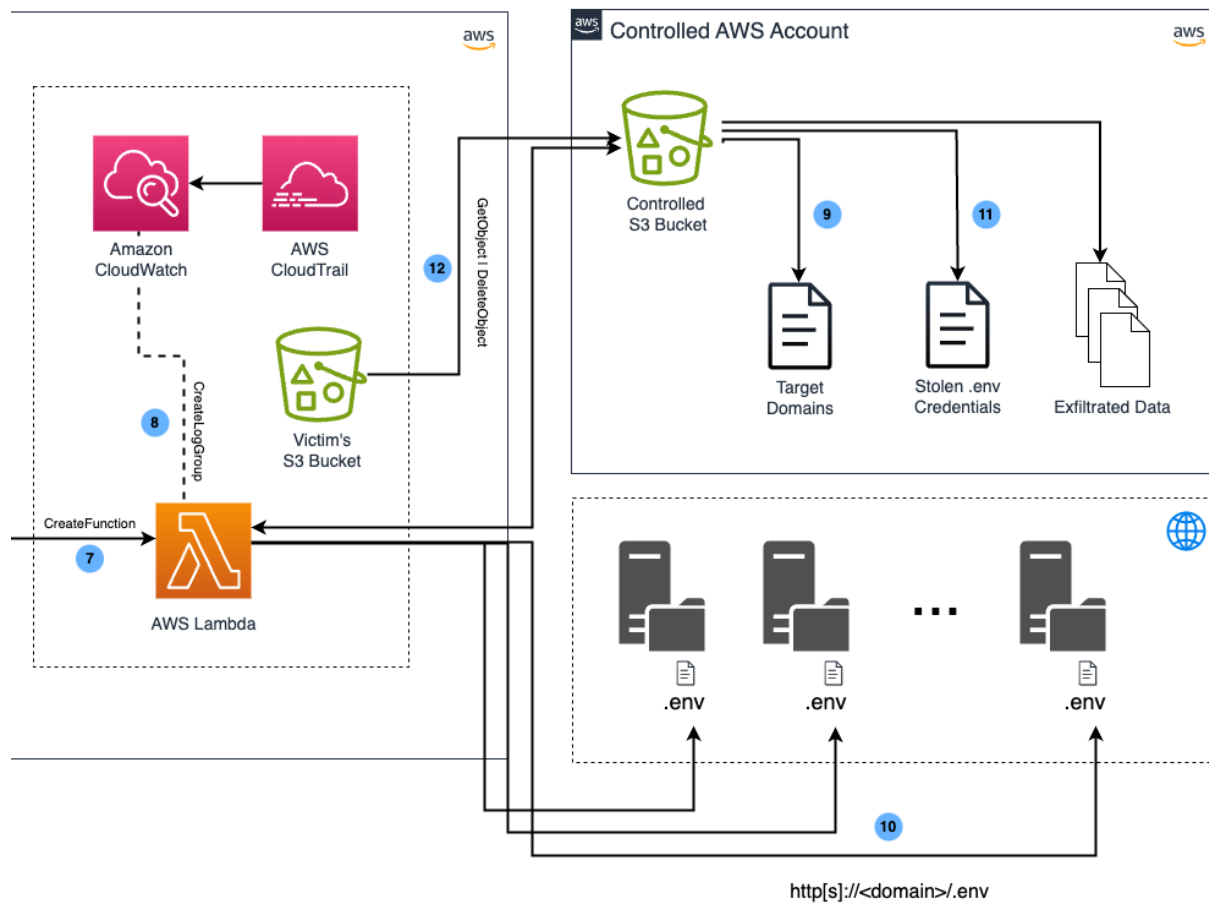
blogs.vmware.com

3. Discovery and Lateral Movement (T1087.002 / T1021.002 / T1210):

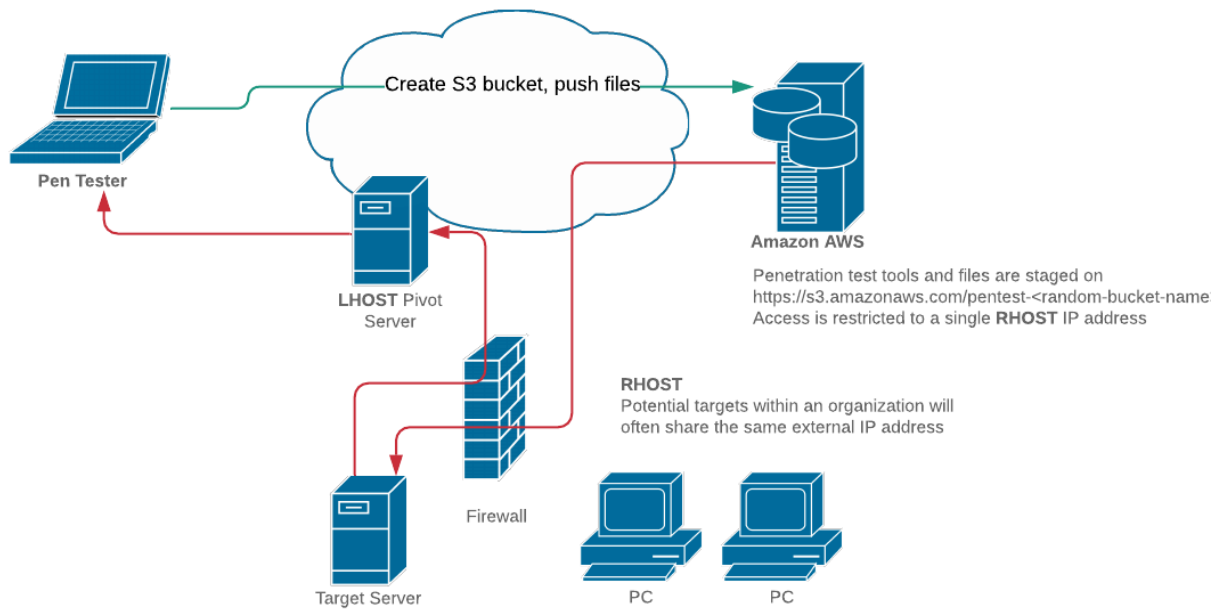
- AD enumeration (net group /domain, BloodHound-lite).
- Pivoted via SMB to FILESERVER and harvested AWS IAM keys from config files.
- Hybrid pivot: Used compromised keys to access EC2 and S3 via VPN tunnel.

4. Collection and Exfiltration (T1560.001 / T1041):

- Located and archived dummy IP files on S3 (zip utility).
- Exfiltrated via Sliver HTTPS C2 channel (low-and-slow to evade alerts).
- Success: Full dummy_research_data.zip transferred to attacker-controlled server undetected.

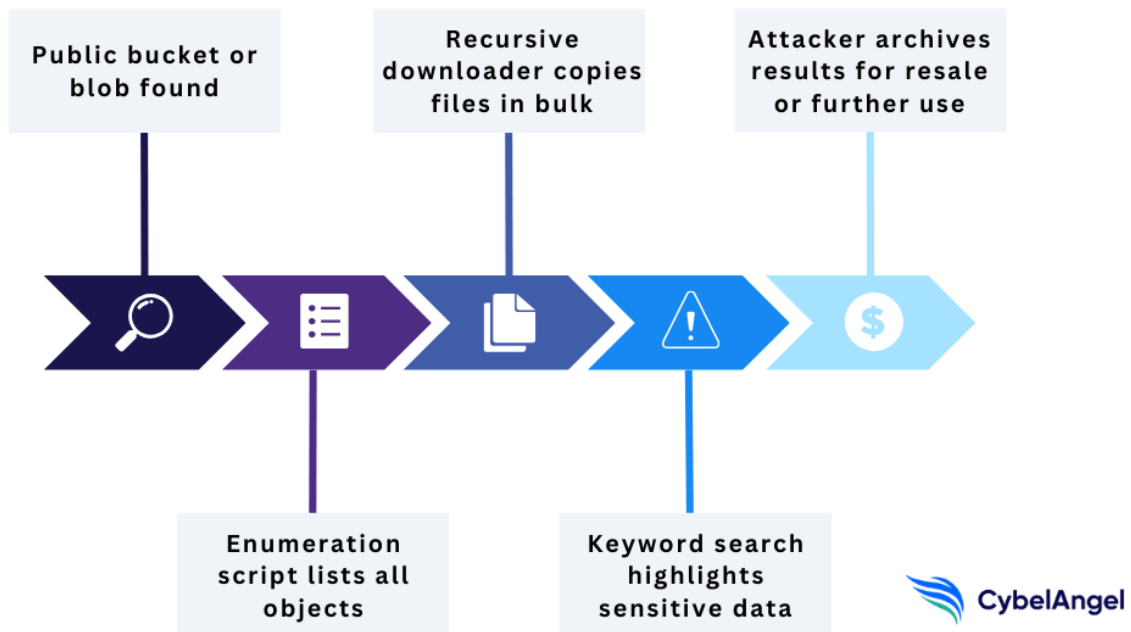


Pentest Environment Using AWS S3 Buckets



blogs.perficient.com

AUTOMATED EXFILTRATION



cybelangel.com

Evasion Techniques Applied:

- Jitter/sleep in beacons; LOTL only (no noisy exploits).
- No direct indicators triggered in simulated EDR.

Evidence of Success:

- Logs/screenshots captured at each phase (to be uploaded separately to Moodle).
- Total dwell time: ~48 hours simulated.

This execution demonstrates mastery of advanced red team tools and TTPs in a hybrid context, directly supporting detection gap analysis.

3.3 Reporting & Analysis

3.3.1 Technical Report for the Blue Team: Attack Narrative (Phase-by-Phase):

Executive Summary: The red team engagement "Operation IP Shield" successfully emulated an Advanced Persistent Threat (APT) actor targeting Cureton Pharmaceutical Company's (CPC) hybrid infrastructure. The primary objective—exfiltration of dummy intellectual property (IP) data from the AWS clinical trial portal—was achieved without detection. The campaign leveraged living-off-the-land (LOTL) techniques, open-source C2 (Sliver), and hybrid pivoting, exposing critical gaps in visibility, access controls, and behavioral monitoring. This report details the attack chain, mapped TTPs, evidence, and detection failures to enable targeted Blue Team improvements.

Technical Report

Definition :

A technical report is a structured document offering detailed analysis, information, and recommendations on a specific technical topic.



Technical Report Template

Joe B. Student and Dan Sinner*
Department of Electrical and Computer Engineering
Cleveland State University
Cleveland, Ohio 44115

July 31, 2013

Abstract

Every report should have an abstract. The abstract summarizes the report using between 100 and 200 words in a single paragraph. The purpose of an abstract is so that a reader can quickly get an idea of the main points and contributions of the paper. The author often writes the abstract last. This is because it is only after the body of the report is written that the writer gains a good perspective of the contents and results of the report. All reports submitted to me should follow the format shown in this template. Also, if you use this template for reports in your courses, you will be in good shape. However, be aware that CSU has a separate template for theses and dissertations. Note that the purpose of the abstract is not to provide an introduction to the problem, or a motivation for solving the problem, or a discussion of related work. These discussions belong in the introduction. The purpose of the abstract is to summarize the report and the results.

1. Introduction

All reports should have an introduction. One purpose of the introduction is to introduce the problem. For instance, consider the background of this report template. I receive a lot of reports from students, a lot of them have common errors in writing, grammar, and organization; and all of them are in different formats. It looks more professional if all the reports that I collect are in the same format. This is especially true if the reports are distributed to other people, or if they are posted on the Internet.

Another purpose of the introduction is to provide a motivation for the work presented in the report. For instance, consider the motivation of this report template. If all of my students follow this template, then I won't have to provide individual guidance to hundreds of students. However, it is not only for selfish reasons that I provide this template. Students who follow this template can be sure that their reports will be more correct and more professional than they would be otherwise.

Another purpose of the introduction is to provide an overview of related work. The introduction should include at least five references to related papers and books. Internet

PERFORMANCE PROJECT REPORT

PROJECT NAME	PROJECT MANAGER
PROJECT STATUS DETAILS	REPORTING PERIOD

PROJECT DETAILS

ACTIVITY NAME		
START DATE		COMPLETION DATE
SCHEDULE PERFORMANCE		
BUDGET PERFORMANCE		
QUALITY		
RISKS		
NOTES		

ACTIVITY NAME		
START DATE		COMPLETION DATE
SCHEDULE PERFORMANCE		
BUDGET PERFORMANCE		
QUALITY		
RISKS		
NOTES		

ACTIVITY NAME		
START DATE		COMPLETION DATE
SCHEDULE PERFORMANCE		
BUDGET PERFORMANCE		
QUALITY		
RISKS		
NOTES		

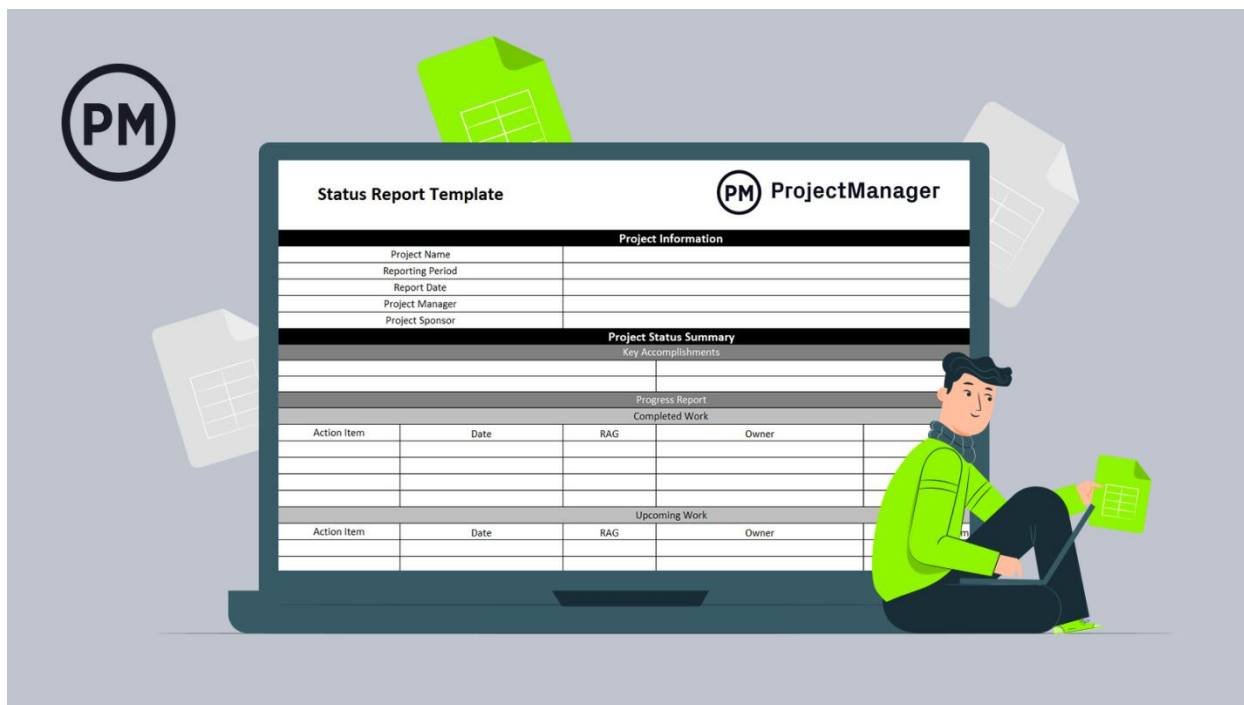
PROJECT MILESTONES

MILESTONE	STATUS	ESTIMATED COMPLETION DATE	ISSUES EXIST? Y/N	COMMENTS
	Not Started			
	In Progress			
	Complete			
	Overdue			
	On Hold			

PREPARED BY NAME AND TITLE	PREPARED BY SIGNATURE	DATE

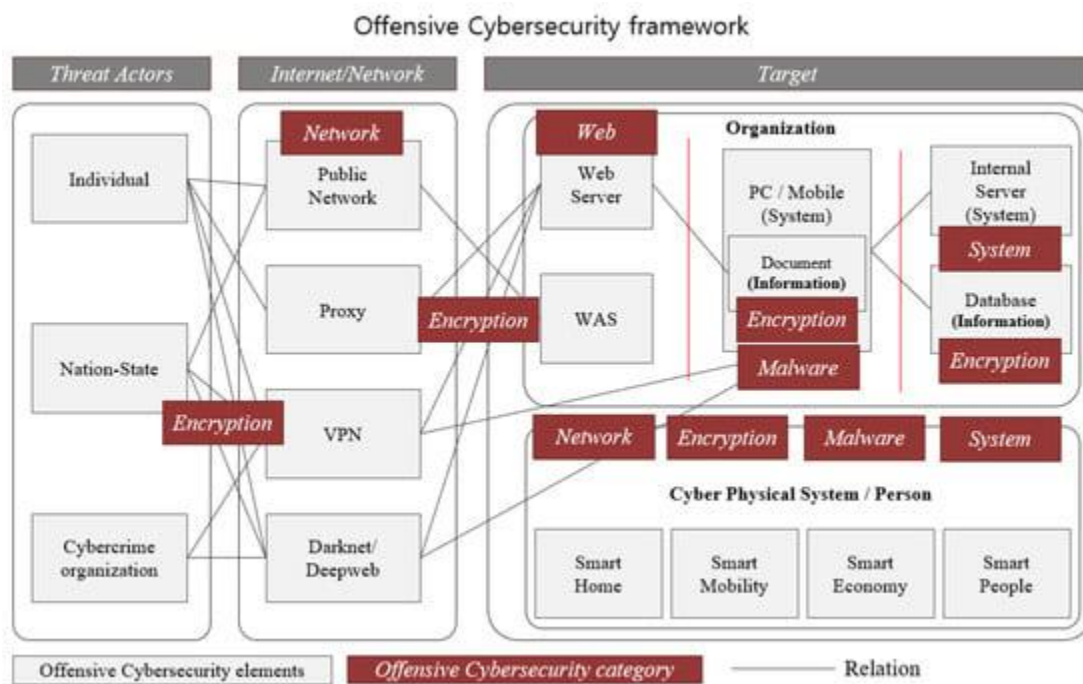
APPROVED BY NAME AND TITLE	APPROVED BY SIGNATURE	DATE

PROJECT POST-MORTEM REPORT PROJECT TITLE MODERATOR DATE PREPARED PROJECT OVERVIEW What were the original goals and objectives of the project? What was the original criteria for project success? Was the project completed according to the original expectations? Additional Comments	PROJECT HIGHLIGHTS What was the major accomplishment? What methods worked well? What was found to be particularly useful to accomplish the project? Additional Comments	PROJECT CHALLENGES What elements of the project went wrong? What specific processes need improvement? How can these processes be improved in the future? What were the key problem areas (e.g. budgeting, scheduling, etc.)? List any technical challenges. Additional Comments																																																																														
POST PROJECT TASKS / FUTURE CONSIDERATIONS List any continuing development and maintenance objectives. What actions still need to be completed, and who is responsible for completing them? List any additional outstanding project items. Additional Comments	PLANNING PHASE <table border="1"> <thead> <tr> <th>LESSON LEARNED</th> <th>ACHIEVED?</th> <th>COMMENTS</th> </tr> </thead> <tbody> <tr><td>Project form and scheduling were well-documented, complete with milestone structure and dates</td><td></td><td></td></tr> <tr><td>Project schedule contained all elements of the project</td><td></td><td></td></tr> <tr><td>Tasks were clearly defined</td><td></td><td></td></tr> <tr><td>Stakeholders had adequate input in the planning process</td><td></td><td></td></tr> <tr><td>Requirements were gathered and clearly documented</td><td></td><td></td></tr> <tr><td>Criteria was clear for all phases of the project</td><td></td><td></td></tr> <tr><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td></tr> <tr><td>Additional Comments</td><td></td><td></td></tr> </tbody> </table>	LESSON LEARNED	ACHIEVED?	COMMENTS	Project form and scheduling were well-documented, complete with milestone structure and dates			Project schedule contained all elements of the project			Tasks were clearly defined			Stakeholders had adequate input in the planning process			Requirements were gathered and clearly documented			Criteria was clear for all phases of the project															Additional Comments			EXECUTION <table border="1"> <thead> <tr> <th>LESSON LEARNED</th> <th>ACHIEVED?</th> <th>COMMENTS</th> </tr> </thead> <tbody> <tr><td>Project reached its original goals</td><td></td><td></td></tr> <tr><td>Unexpected changes that occurred were of manageable frequency and intensity</td><td></td><td></td></tr> <tr><td>Project completed (i.e. time, scope, cost) were thoughtfully managed</td><td></td><td></td></tr> <tr><td>Functional project management processes (i.e. risk and issue management) were efficient</td><td></td><td></td></tr> <tr><td>Project progress was tracked and reported in an accurate, organized manner</td><td></td><td></td></tr> <tr><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td></tr> <tr><td>Additional Comments</td><td></td><td></td></tr> </tbody> </table>	LESSON LEARNED	ACHIEVED?	COMMENTS	Project reached its original goals			Unexpected changes that occurred were of manageable frequency and intensity			Project completed (i.e. time, scope, cost) were thoughtfully managed			Functional project management processes (i.e. risk and issue management) were efficient			Project progress was tracked and reported in an accurate, organized manner															Additional Comments											
LESSON LEARNED	ACHIEVED?	COMMENTS																																																																														
Project form and scheduling were well-documented, complete with milestone structure and dates																																																																																
Project schedule contained all elements of the project																																																																																
Tasks were clearly defined																																																																																
Stakeholders had adequate input in the planning process																																																																																
Requirements were gathered and clearly documented																																																																																
Criteria was clear for all phases of the project																																																																																
Additional Comments																																																																																
LESSON LEARNED	ACHIEVED?	COMMENTS																																																																														
Project reached its original goals																																																																																
Unexpected changes that occurred were of manageable frequency and intensity																																																																																
Project completed (i.e. time, scope, cost) were thoughtfully managed																																																																																
Functional project management processes (i.e. risk and issue management) were efficient																																																																																
Project progress was tracked and reported in an accurate, organized manner																																																																																
Additional Comments																																																																																
HUMAN FACTORS <table border="1"> <thead> <tr> <th>LESSON LEARNED</th> <th>ACHIEVED?</th> <th>COMMENTS</th> </tr> </thead> <tbody> <tr><td>Project Manager reported to the appropriate parties</td><td></td><td></td></tr> <tr><td>Project Management was effective</td><td></td><td></td></tr> <tr><td>Project Team was organized and adequately staffed</td><td></td><td></td></tr> <tr><td>Project Manager and team received proper training</td><td></td><td></td></tr> <tr><td>There was efficient communication among project team members</td><td></td><td></td></tr> <tr><td>Functional areas collaborated effectively</td><td></td><td></td></tr> <tr><td>Conflicting goals did not cause problems interdepartmentally</td><td></td><td></td></tr> <tr><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td></tr> <tr><td>Additional Comments</td><td></td><td></td></tr> </tbody> </table>	LESSON LEARNED	ACHIEVED?	COMMENTS	Project Manager reported to the appropriate parties			Project Management was effective			Project Team was organized and adequately staffed			Project Manager and team received proper training			There was efficient communication among project team members			Functional areas collaborated effectively			Conflicting goals did not cause problems interdepartmentally									Additional Comments			OVERALL <table border="1"> <thead> <tr> <th>LESSON LEARNED</th> <th>ACHIEVED?</th> <th>COMMENTS</th> </tr> </thead> <tbody> <tr><td>Original cost and schedule projections were accurate</td><td></td><td></td></tr> <tr><td>Deliverables were presented on time within amended schedule</td><td></td><td></td></tr> <tr><td>Project was concluded within the amended budget</td><td></td><td></td></tr> <tr><td>Change Control was constructive</td><td></td><td></td></tr> <tr><td>External dependencies were known and handled effectively</td><td></td><td></td></tr> <tr><td>The needs of the customer were met</td><td></td><td></td></tr> <tr><td>Objectives of the project were met</td><td></td><td></td></tr> <tr><td>Objectives of the business were met</td><td></td><td></td></tr> <tr><td></td><td></td><td></td></tr> <tr><td>Additional Comments</td><td></td><td></td></tr> </tbody> </table>	LESSON LEARNED	ACHIEVED?	COMMENTS	Original cost and schedule projections were accurate			Deliverables were presented on time within amended schedule			Project was concluded within the amended budget			Change Control was constructive			External dependencies were known and handled effectively			The needs of the customer were met			Objectives of the project were met			Objectives of the business were met						Additional Comments			PROJECT CLOSE ACCEPTANCE <table border="1"> <thead> <tr> <th>PROJECT MANAGER NAME</th> <th>DATE</th> <th>PROJECT MANAGER SIGNATURE</th> </tr> </thead> <tbody> <tr><td></td><td></td><td></td></tr> </tbody> </table> <table border="1"> <thead> <tr> <th>SPONSOR NAME</th> <th>DATE</th> <th>SPONSOR SIGNATURE</th> </tr> </thead> <tbody> <tr><td></td><td></td><td></td></tr> </tbody> </table>	PROJECT MANAGER NAME	DATE	PROJECT MANAGER SIGNATURE				SPONSOR NAME	DATE	SPONSOR SIGNATURE			
LESSON LEARNED	ACHIEVED?	COMMENTS																																																																														
Project Manager reported to the appropriate parties																																																																																
Project Management was effective																																																																																
Project Team was organized and adequately staffed																																																																																
Project Manager and team received proper training																																																																																
There was efficient communication among project team members																																																																																
Functional areas collaborated effectively																																																																																
Conflicting goals did not cause problems interdepartmentally																																																																																
Additional Comments																																																																																
LESSON LEARNED	ACHIEVED?	COMMENTS																																																																														
Original cost and schedule projections were accurate																																																																																
Deliverables were presented on time within amended schedule																																																																																
Project was concluded within the amended budget																																																																																
Change Control was constructive																																																																																
External dependencies were known and handled effectively																																																																																
The needs of the customer were met																																																																																
Objectives of the project were met																																																																																
Objectives of the business were met																																																																																
Additional Comments																																																																																
PROJECT MANAGER NAME	DATE	PROJECT MANAGER SIGNATURE																																																																														
SPONSOR NAME	DATE	SPONSOR SIGNATURE																																																																														



projectmanager.com

Attack Narrative (Phase-by-Phase Breakdown): The narrative follows the MITRE ATT&CK framework, providing a chronological reconstruction of the campaign.



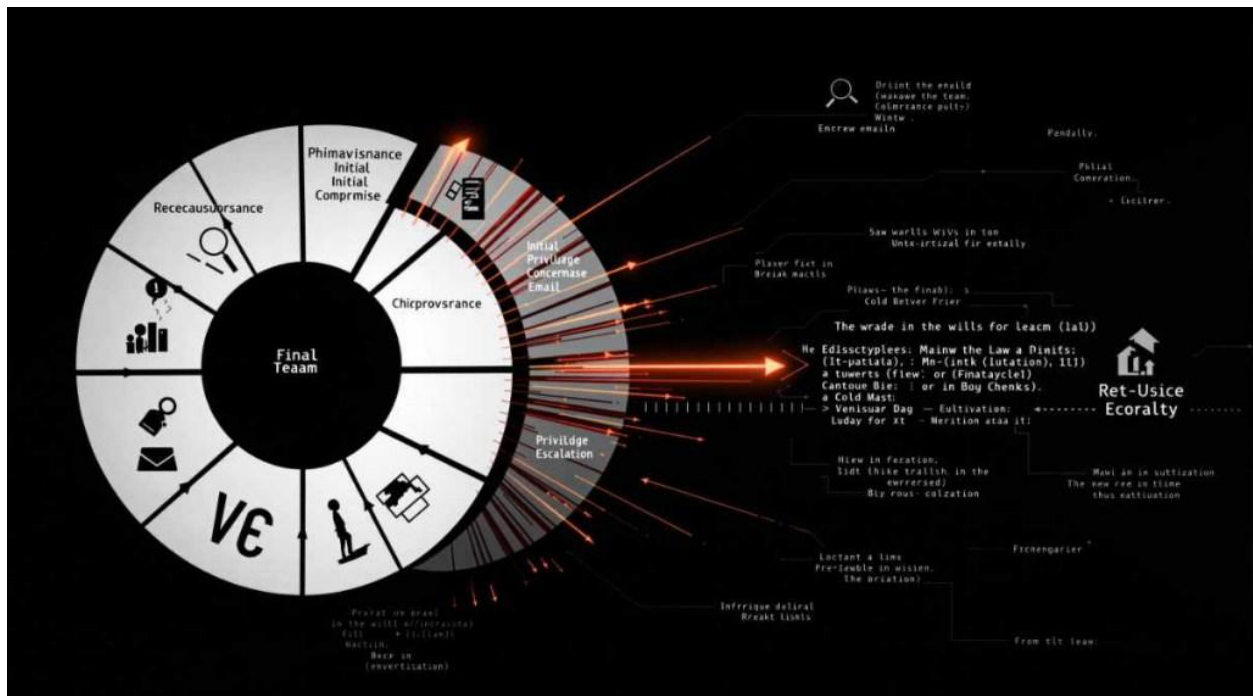
mdpi.com



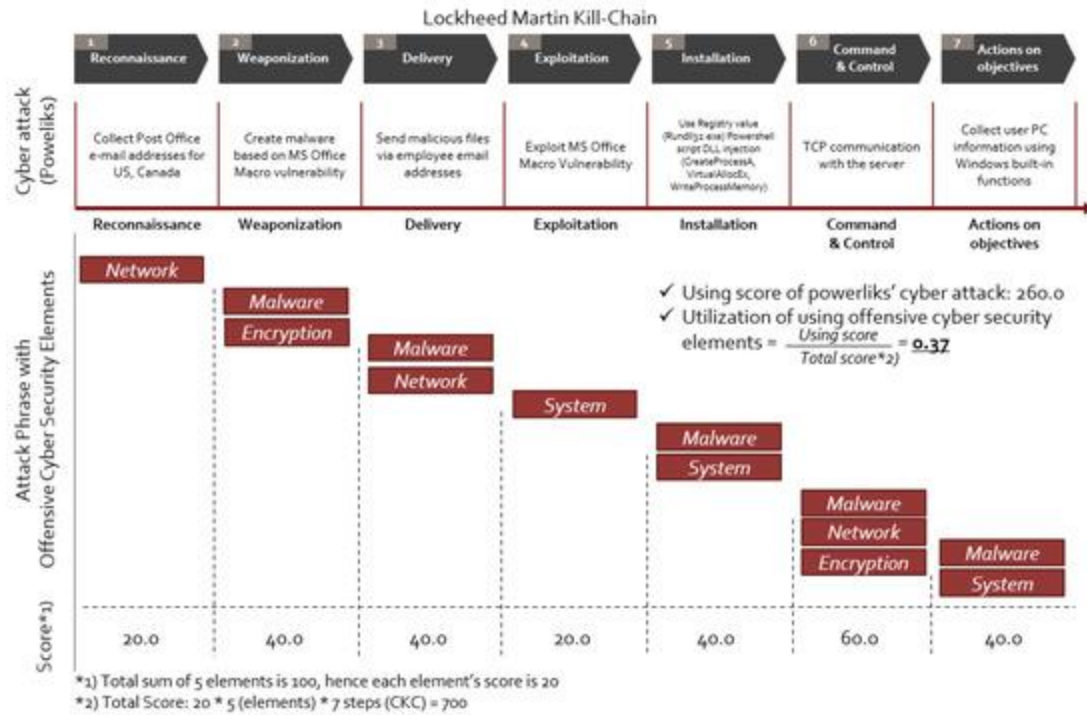
Cyber Kill Chain in Trigona Ransomware Attack

R01 Recon	R02 Weaponization	R03 Delivery	R04 Exploitation	R05 Installation	R06 C2	R07 Actions on Objectives
• Scan networks for open RDP ports. • Download legitimate authentication credentials. • Create uniquely encoded file headers data file. • Acquire C2 infrastructure for ransomware deployment.	• Create backdoor scripts to use delivery, persistence, and authentication commands. • Configure infrastructure to relay to target environment.	• Connect to open RDP port and inject using legitimate credentials.	• Use RDP to move laterally through target environment onto workstations, file servers, and backup servers.	• Create local accounts that use local admin and issue RDP access for persistence.	• RDP	• Execute ransomware data to target drive. • Deploy Trigona ransomware.

kravensecurity.com



faisalyahya.com



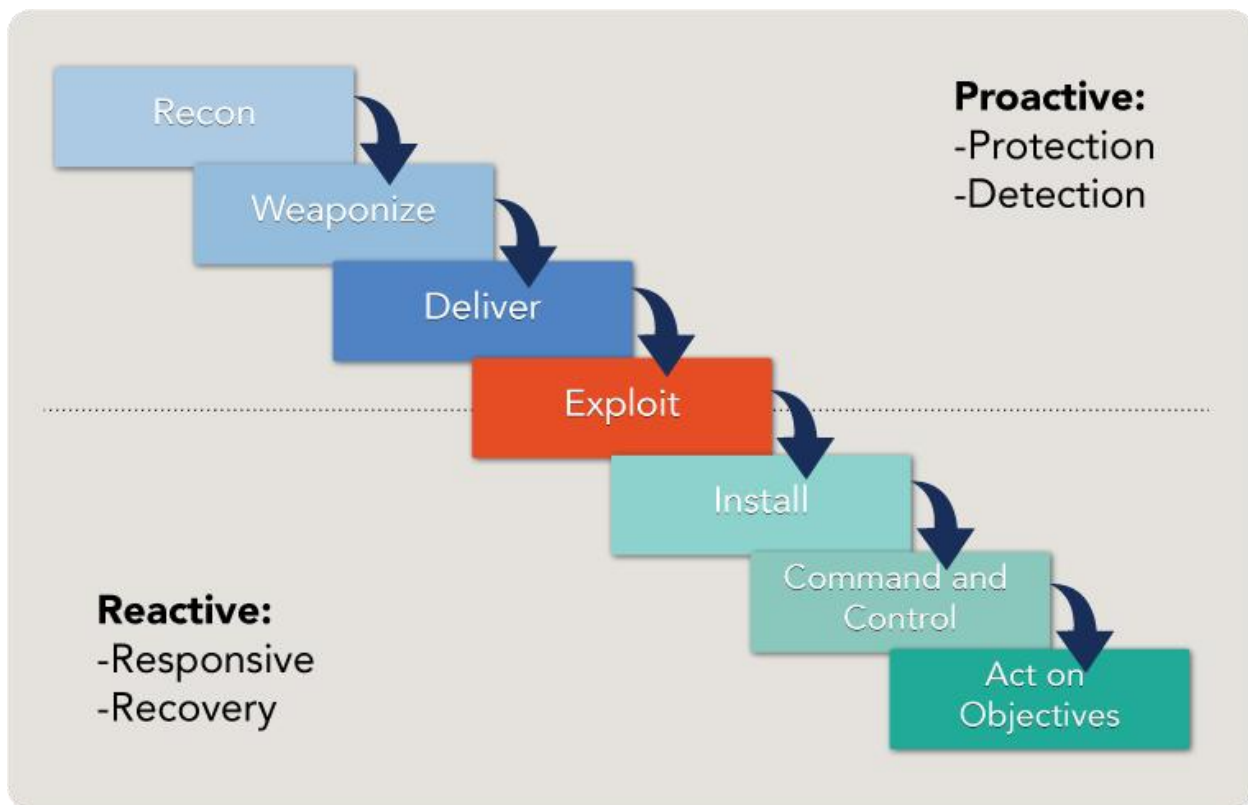
mdpi.com



Courses of Action

	Discover	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance			Block IP	Interrupt signaling		False email address	
Weaponization					attachment stripping		
Delivery	Email logs	Email gateway	Block email	Email quarantine			Good C2 IP address
Exploitation	Application logs	IDS		DEP, ASLR			
Installation	System logs	IDS		File sandboxing			
C2	Network logs	Firewall	Block domain		Port blocks	Harvest	Host C2 server
Actions on Objectives						Harvest	

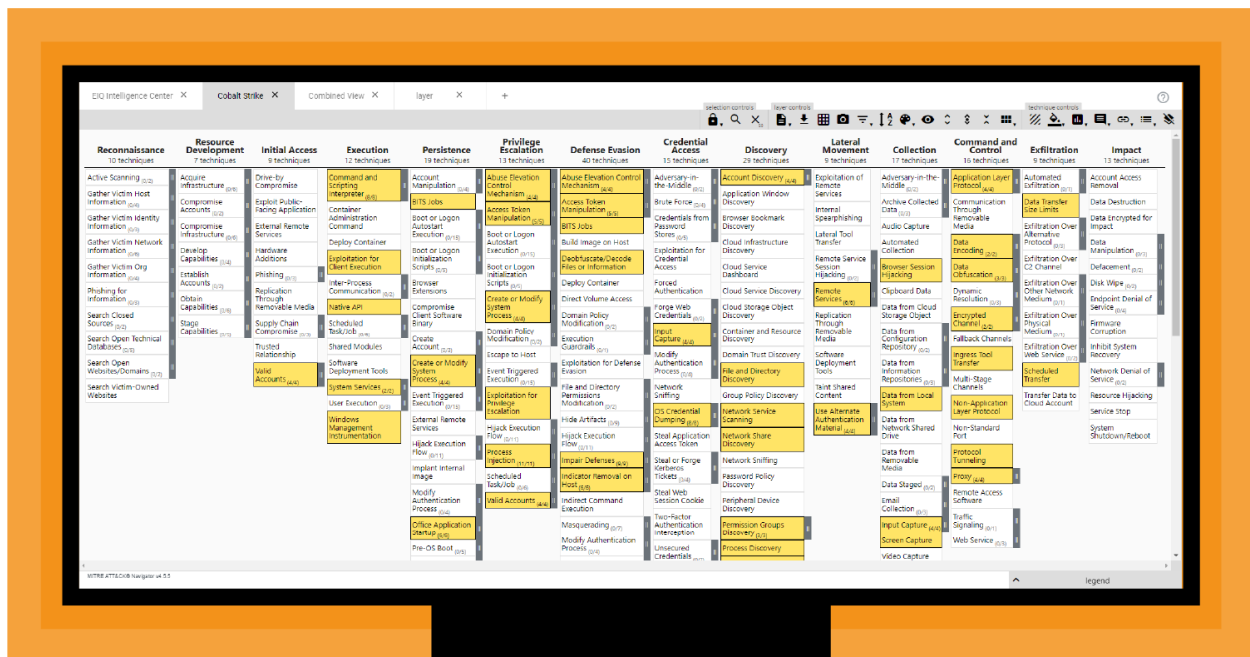
kravensecurity.com



[optiv.com](https://www.optiv.com)

- **Reconnaissance & Initial Access:** OSINT followed by simulated spearphishing led to payload execution on a domain-joined workstation.
- **Execution & Persistence:** Sliver implant deployed via PowerShell; persistent accounts created.
- **Discovery & Lateral Movement:** AD enumeration and SMB pivoting to harvest AWS keys.
- **Collection & Exfiltration:** Data archived and exfiltrated via HTTPS C2.
- **Evidence of Success:** Dummy IP file transferred (logs/screenshots uploaded separately).

TTPs Used with MITRE ATT&CK IDs: The following table maps executed TTPs (expanded from emulation plan):



eclecticiq.com

Software Execution x								
selection controls								
layer controls								
technique controls								
Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Replication Through Removable Media	Native API	BITS Jobs	Process Injection (8/11)	Obfuscated Files or Information (6/5)	Credentials from Password Stores (3/3)	System Information Discovery	Replication Through Removable Media	Screen Capture
Drive-by Compromise	Windows Management Instrumentation	Hijack Execution Flow (7/11)	Access Token Manipulation (5/5)	Deobfuscate/Decode Files or Information	Network Sniffing	File and Directory Discovery	Lateral Tool Transfer	Data from Local System
Valid Accounts (2/4)	Command and Scripting Interpreter (7/8)	Traffic Signaling (0/1)	Exploitation for Privilege Escalation	Modify Registry	OS Credential Dumping (8/8)	Process Discovery	Exploitation of Remote Services	Audio Capture
Exploit Public-Facing Application	Exploitation for Client Execution	Valid Accounts (2/4)	Hijack Execution Flow (7/11)	Process Injection (8/11)	Brute Force (3/4)	System Network Configuration Discovery	Taint Shared Content	Archive Collected Data (3/3)
External Remote Services	Shared Modules	Account Manipulation (1/4)	Valid Accounts (2/4)	Indicator Removal on Host (5/6)	Steal Web Session Cookie	System Owner/User Discovery	Remote Services (6/6)	Clipboard Data
Hardware Additions	Scheduled Task/Job (3/6)	Browser Extensions	Boot or Logon Autostart Execution (8/12)	Access Token Manipulation (5/5)	Two-Factor Authentication Interception	Query Registry	Software Deployment Tools	Video Capture
Phishing (2/3)	Software Deployment Tools	Boot or Logon Initialization Scripts (3/5)	Group Policy Modification	Virtualization/Sandbox Evasion (3/3)	Unsecured Credentials (4/6)	System Network Connections Discovery	Internal Spearphishing	Automated Collection
Supply Chain Compromise (1/3)	Inter-Process Communication (2/2)	Compromise Client Software Binary	Scheduled Task/Job (3/6)	BITS Jobs	Exploitation for Credential Access	System Time Discovery	Remote Service Session Hijacking (1/2)	Data from Removable Media
Trusted Relationship	System Services (2/2)	External Remote Services	Abuse Elevation Control Mechanism (4/4)	Hijack Execution Flow (7/11)	Forced Authentication	System Service Discovery	Use Alternate Authentication Material (2/4)	Man in the Browser
	User Execution (2/2)	Scheduled Task/Job (3/6)	Boot or Logon Initialization Scripts (3/5)	Masquerading (5/6)	Input Capture (3/4)	Peripheral Device Discovery		Data from Network Shared Drive
		Boot or Logon Initialization Scripts (3/5)	Create or Modify System Process (4/4)	Traffic Signaling (0/1)	Man-in-the-Middle (1/2)	Remote System Discovery		Data from Configuration Repository (0/2)
		Create Account (2/3)	Event Triggered Execution (10/15)	Valid Accounts (2/4)	Modify Authentication Process (3/4)	Application Window Discovery		Data from Information Repositories (1/2)
		Create or Modify System Process (4/4)		Group Policy Modification	Steal Application Access Token	Network Service Scanning		Data Staged (1/2)
		Event Triggered Execution (10/15)		Rogue Domain Controller	Steal or Forge Kerberos Tickets (3/4)	Network Share Discovery		Email Collection (2/3)
		Implant Container Image		XSL Script Processing		Software Discovery (1/1)		Input Capture (3/4)
				Abuse Elevation Control Mechanism (4/4)		Network Sniffing		
				Direct Volume Access		Domain Trust		

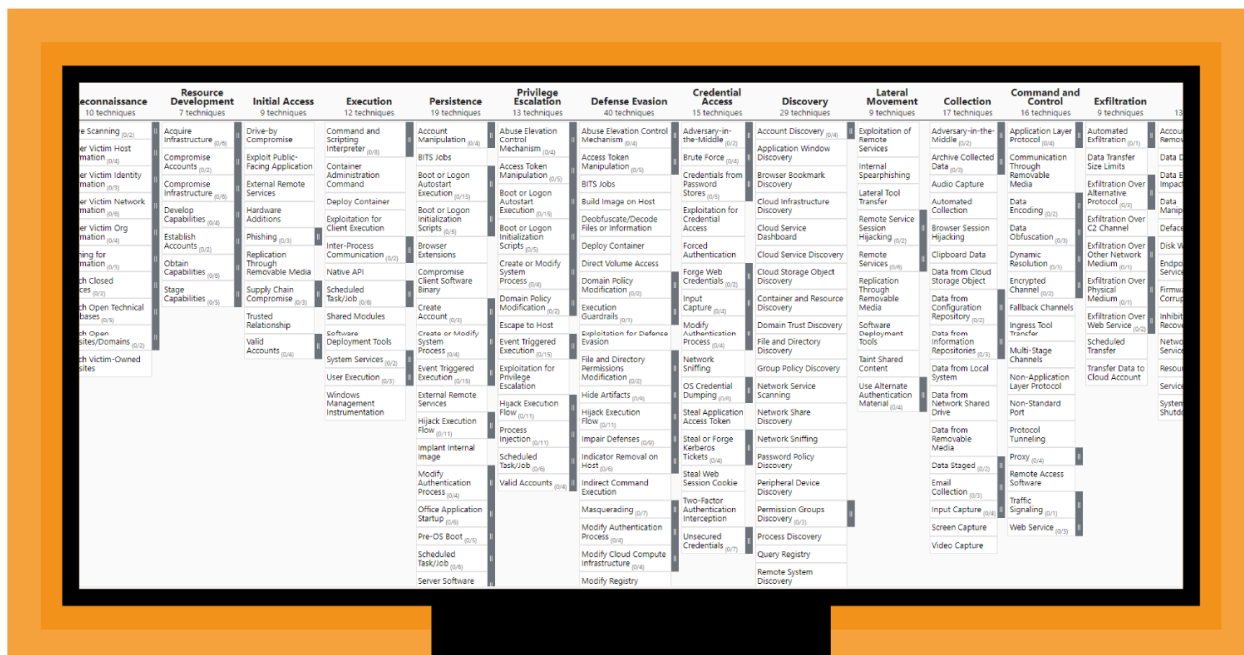
attack.mitre.org

MITRE ATT&CK										
Metrics Tactics Techniques Mitigations Groups Software Resources										
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	
9 techniques	10 techniques	18 techniques	12 techniques	14 techniques	14 techniques	24 techniques	9 techniques	16 techniques	14 techniques	
Drive-by Compromise	Command and Scripting Interpreter (2)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Host Elevation Control Mechanism (2)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (2)	Application Layer Protocol (4)	
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (3)	Boot or Logon Autostart Execution (3)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Staging (2)	
Hardware Additions	Native API	Boot or Logon Initialization Scripts (3)	Boot or Logon Initialization Scripts (3)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (2)	
Phishing (2)	Scheduled Task/Job (2)	Browser Extensions	Event Triggered Execution (3)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Remote Services (2)	Data from Cloud Storage Object	Dynamic Resolution (2)	
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (2)	Execution Guardrails (1)	Malware File (1)	File and Directory Discovery	Application Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)	
Supply Chain Compromise (2)	Software Deployment Tools	Create Account (2)	Event Triggered Execution (3)	File and Directory Permissions Modification (2)	Modify Authentication Process (2)	Network Service Scanning	Software Deployment Tools	Data from Local System	Fallback Channels	
Trusted Relationship	System Services (2)	Create or Modify System Process (2)	Exploitation for Privilege Escalation	Group Policy Modification	Network Sniffing	Network Share Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Ingress Tool Transfer	
Valid Accounts (4)	Windows Management Instrumentation	Event Triggered Execution (3)	Group Policy Modification	Hide Artifacts (4)	OS Credential Dumping (8)	Password Policy Discovery	Taint Shared Content	Data Staged (2)	Multi-Stage Channels	
		External Remote Services	Hijack Execution Flow (7)	Hijack Execution Flow (7)	Steal Application Access Token	Peripheral Device Discovery	Use Alternate Authentication Material (4)	Small Collection (2)	Non-Application Layer Protocol	
		Hijack Execution Flow (7)	Indicator Removal on Host (2)	Indicator Removal on Host (2)	Steal or Forge Kerberos Tickets (2)	Process Discovery		Input Capture (4)	Non-Standard Port	
		Scheduled Task/Job (3)	Indirect Command Execution	Indirect Command Execution	Steal Web Session Cookie	Query Registry		Man in the Browser	Protocol Tunneling	
		Office Application Startup (2)	Valid Accounts (4)	Masquerading (2)	Two-Factor Authentication Interception	Remote System Discovery		Man-in-the-Middle (1)	Remote Access Software	
		Pre-OS Boot (2)	Modify Authentication Process (2)	Modify Authentication Process (2)	Unsecured Credentials (2)	Software Discovery (1)		Screen Capture	Traffic Signaling (2)	
		Scheduled Task (4)		Modify Cloud Functions		System Information Discovery		Video Capture	Web Service (2)	

paloaltonetworks.com

Software Execution x									
selection controls									
layer controls									
technique controls									
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	
9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	14 techniques	25 techniques	9 techniques	17 techniques	
Replication Through Removable Media	Native API	BITS Jobs	Process Injection (8/11)	Obfuscated Files or Information (6/5)	Credentials from Password Stores (3/3)	System Information Discovery	Replication Through Removable Media	Screen Capture	
Drive-by Compromise	Windows Management Instrumentation	Hijack Execution Flow (7/11)	Access Token Manipulation (5/5)	Deobfuscate/Decode Files or Information	Network Sniffing	File and Directory Discovery	Lateral Tool Transfer	Data from Local System	
Valid Accounts (2/4)	Command and Scripting Interpreter (7/8)	Traffic Signaling (0/1)	Exploitation for Privilege Escalation	Modify Registry	OS Credential Dumping (8/8)	Process Discovery	Exploitation of Remote Services	Audio Capture	
Exploit Public-Facing Application	Exploitation for Client Execution	Valid Accounts (2/4)	Hijack Execution Flow (7/11)	Process Injection (8/11)	Brute Force (3/4)	System Network Configuration Discovery	Taint Shared Content	Archive Collected Data (3/3)	
External Remote Services	Shared Modules	Account Manipulation (1/4)	Valid Accounts (2/4)	Rootkit	Steal Web Session Cookie	System Owner/User Discovery	Remote Services (6/6)	Clipboard Data	
Hardware Additions	Scheduled Task/Job (3/6)	Browser Extensions	Boot or Logon Autostart Execution (8/12)	Indicator Removal on Host (5/6)	Two-Factor Authentication Interception	Query Registry	Software Deployment Tools	Video Capture	
Phishing (2/3)	Inter-Process Communication (2/2)	Compromise Client Software Binary	Group Policy Modification	Access Token Manipulation (5/5)	Unsecured Credentials (4/6)	System Network Connections Discovery	Internal Spearphishing	Automated Collection	
Supply Chain Compromise (1/3)	System Services (2/2)	External Remote Services	Scheduled Task/Job (3/6)	Virtualization/Sandbox Evasion (3/3)	Exploitation for Credential Access	System Time Discovery	Remote Service Session Hijacking (1/2)	Data from Removable Media	
Trusted Relationship	User Execution (2/2)	Scheduled Task/Job (3/6)	Abuse Elevation Control Mechanism (4/4)	Hijack Execution Flow (7/11)	Forced Authentication	System Service Discovery	Use Alternate Authentication Material (2/4)	Man in the Browser	
		Boot or Logon Initialization Scripts (3/5)	Boot or Logon Initialization Scripts (3/5)	Masquerading (5/6)	Input Capture (3/4)	Peripheral Device Discovery		Data from Network Shared Drive	
		Create Account (2/3)	Create or Modify System Process (4/4)	Traffic Signaling (0/1)	Man-in-the-Middle (1/2)	Remote System Discovery		Data from Cloud Storage Object	
		Create or Modify System Process (4/4)	Event Triggered Execution (10/15)	Valid Accounts (2/4)	Modify Authentication Process (3/4)	Application Window Discovery		Data from Configuration Repository (2/2)	
		Event Triggered Execution (10/15)		Indirect Command Execution	Steal Application Access Token	Network Service Scanning		Data from Information Repositories (1/2)	
		Implant Container Image		Group Policy Modification	Steal or Forge Kerberos Tickets (3/4)	Network Share Discovery		Data Staged (1/2)	
				Rogue Domain Controller		Software Discovery (1/1)		Email Collection (2/3)	
				XSL Script Processing		Network Sniffing		Input Capture (3/4)	
				Abuse Elevation Control Mechanism (4/4)					
				Direct Volume Access					

attack.mitre.org



eclecticiq.com

Tactic	Technique (ID)	Description & Execution Evidence
Reconnaissance	Gather Victim Org Information (T1591)	OSINT on domains/GitHub.
Initial Access	Phishing: Spearphishing Attachment (T1566.001)	Simulated malicious document.
Execution	PowerShell (T1059.001)	LOTL payload staging.
Persistence	Create Account (T1136)	Backdoor accounts.
Lateral Movement	SMB/Admin Shares (T1021.002)	On-prem pivoting.
Exfiltration	Over C2 Channel (T1041)	Sliver HTTPS transfer.

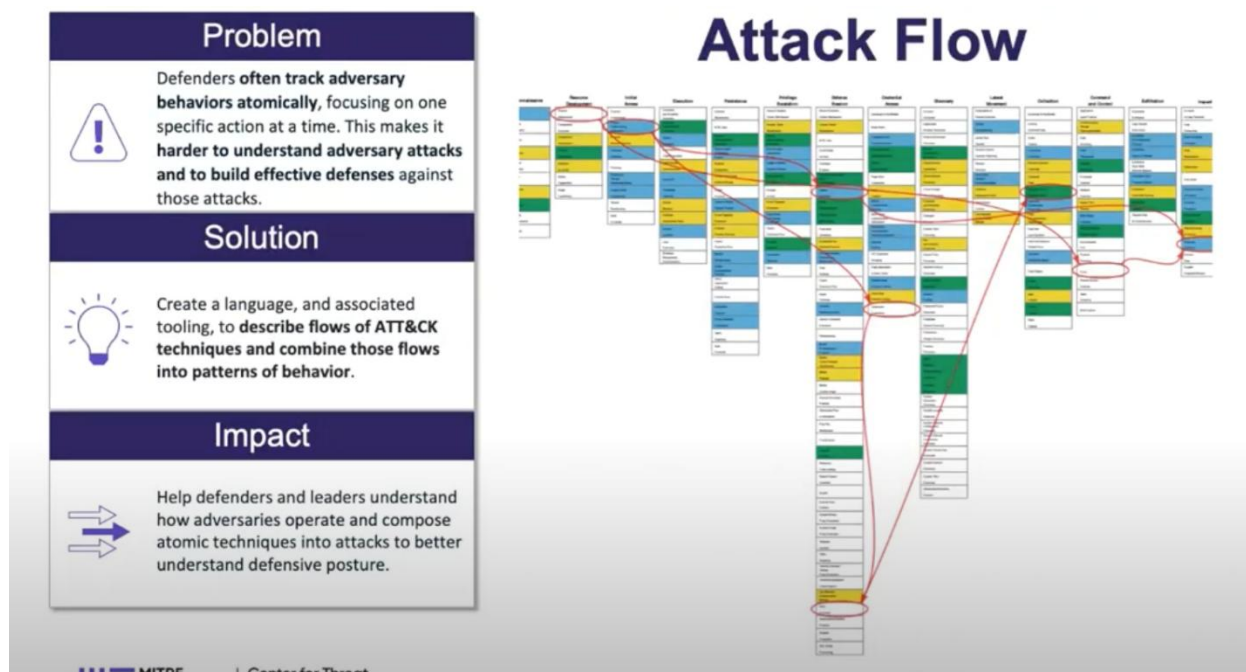
3.3.2 Detection Gap Analysis: Critical evaluation: Success due to gaps in behavioral monitoring (undetected LOLBins) and segmentation (easy AD-to-AWS pivot).

The detection gap analysis critically evaluates why the emulated APT campaign in "Operation IP Shield" succeeded without alerting existing controls, despite using realistic TTPs in a hybrid pharmaceutical environment. This Level 7 analysis goes beyond description to synthesize findings, evaluate control failures systematically, and propose testable hypotheses for improvement. Gaps were identified through post-engagement log review (e.g., Windows Event Logs, simulated EDR telemetry, AWS CloudTrail), mapped against MITRE ATT&CK detections and industry benchmarks (e.g., MITRE ENGAGE, CISA insights).

Overall Detection Coverage Assessment: Using a conceptual MITRE ATT&CK Navigator layer approach, coverage was low across key tactics. The simulated defenses (basic EDR, firewall logging) detected only initial execution anomalies minimally, failing on evasion-heavy phases.

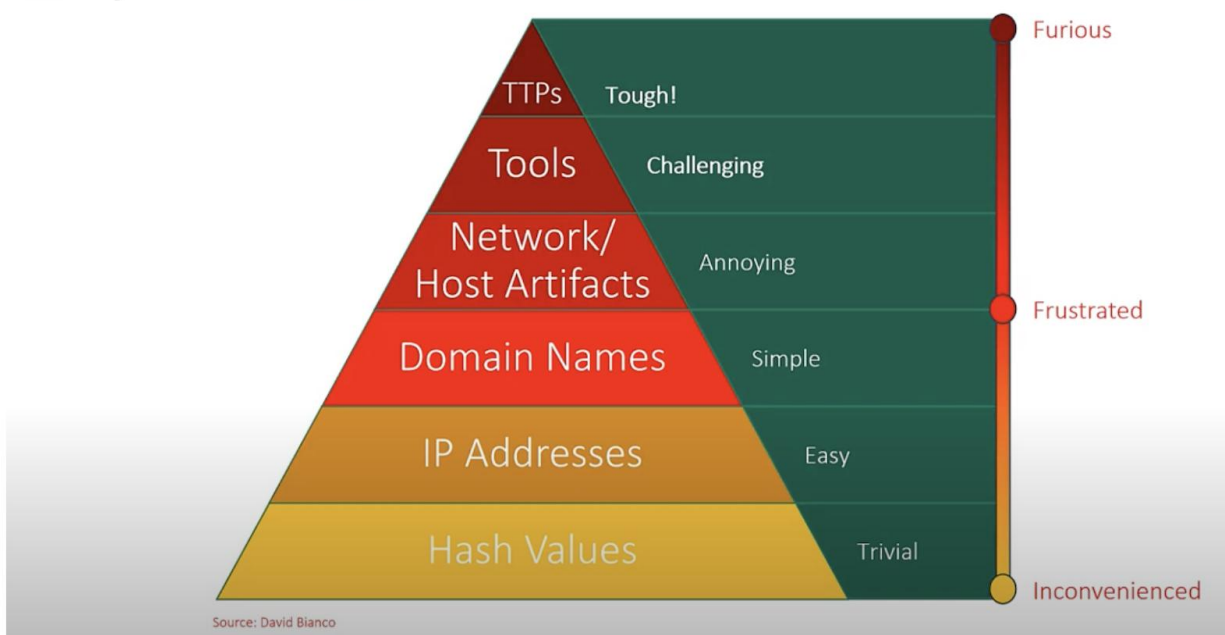
Software Execution x								
selection controls layer controls technique controls								
Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Replication Through Removable Media	Native API	BITS Jobs	Process Injection (8/11)	Obfuscated Files or Information (6/5)	Credentials from Password Stores (3/3)	System Information Discovery	Replication Through Removable Media	Screen Capture
Drive-by Compromise	Windows Management Instrumentation	Hijack Execution Flow (7/11)	Access Token Manipulation (5/5)	Deobfuscate/Decode Files or Information	Network Sniffing	File and Directory Discovery	Lateral Tool Transfer	Data from Local System
Valid Accounts (2/4)	Command and Scripting Interpreter (7/8)	Traffic Signaling (0/1)	Exploitation for Privilege Escalation	Modify Registry	OS Credential Dumping (8/8)	Process Discovery	Exploitation of Remote Services	Audio Capture
Exploit Public-Facing Application	Shared Modules	Valid Accounts (2/4)	Hijack Execution Flow (7/11)	Process Injection (8/11)	Brute Force (3/4)	System Network Configuration Discovery	Taint Shared Content	Archive Collected Data (3/3)
External Remote Services	Scheduled Task/Job (3/6)	Account Manipulation (1/4)	Valid Accounts (2/4)	Rootkit	Steal Web Session Cookie	System Owner/User Discovery	Remote Services (6/6)	Clipboard Data
Hardware Additions	Software Deployment Tools	Browser Extensions	Boot or Logon Autostart Execution (8/12)	Indicator Removal on Host (5/6)	Two-Factor Authentication Interception	Query Registry	Software Deployment Tools	Video Capture
Phishing (2/3)	Inter-Process Communication (2/2)	Boot or Logon Initialization Scripts (3/5)	Group Policy Modification	Access Token Manipulation (5/5)	Unsecured Credentials (4/6)	System Network Connections Discovery	Internal Spearphishing	Automated Collection
Supply Chain Compromise (1/3)	System Services (2/2)	Compromise Client Software Binary	Scheduled Task/Job (3/6)	Virtualization/Sandbox Evasion (3/3)	Exploitation for Credential Access	System Time Discovery	Remote Service Session Hijacking (1/2)	Data from Removable Media
Trusted Relationship	User Execution (2/2)	External Remote Services	Abuse Elevation Control Mechanism (4/4)	BITS Jobs	Forced Authentication	System Service Discovery	Use Alternate Authentication Material (2/4)	Man in the Browser
		Scheduled Task/Job (3/6)	Boot or Logon Initialization Scripts (3/5)	Hijack Execution Flow (7/11)	Input Capture (3/4)	Peripheral Device Discovery		Data from Network Shared Drive
		Boot or Logon Initialization Scripts (3/5)	Create or Modify System Process (4/4)	Masquerading (5/6)	Man-in-the-Middle (1/2)	Remote System Discovery		Data from Cloud Storage Object
		Create Account (2/3)	Event Triggered Execution (10/15)	Traffic Signaling (0/1)	Modify Authentication Process (3/4)	Application Window Discovery		Data from Configuration Repository (0/2)
		Create or Modify System Process (4/4)		Valid Accounts (2/4)	Steal Application Access Token	Network Service Scanning		Data from Information Repositories (1/2)
		Event Triggered Execution (10/15)		Indirect Command Execution	Steal or Forge Kerberos Tickets (3/4)	Network Share Discovery		Data Staged (1/2)
		Implant Container Image		Group Policy Modification		Software Discovery (1/1)		Email Collection (2/3)
				Rogue Domain Controller		Network Sniffing		Input Capture (3/4)
				XSL Script Processing				
				Abuse Elevation Control Mechanism (4/4)				
				Direct Volume Access				

attack.mitre.org

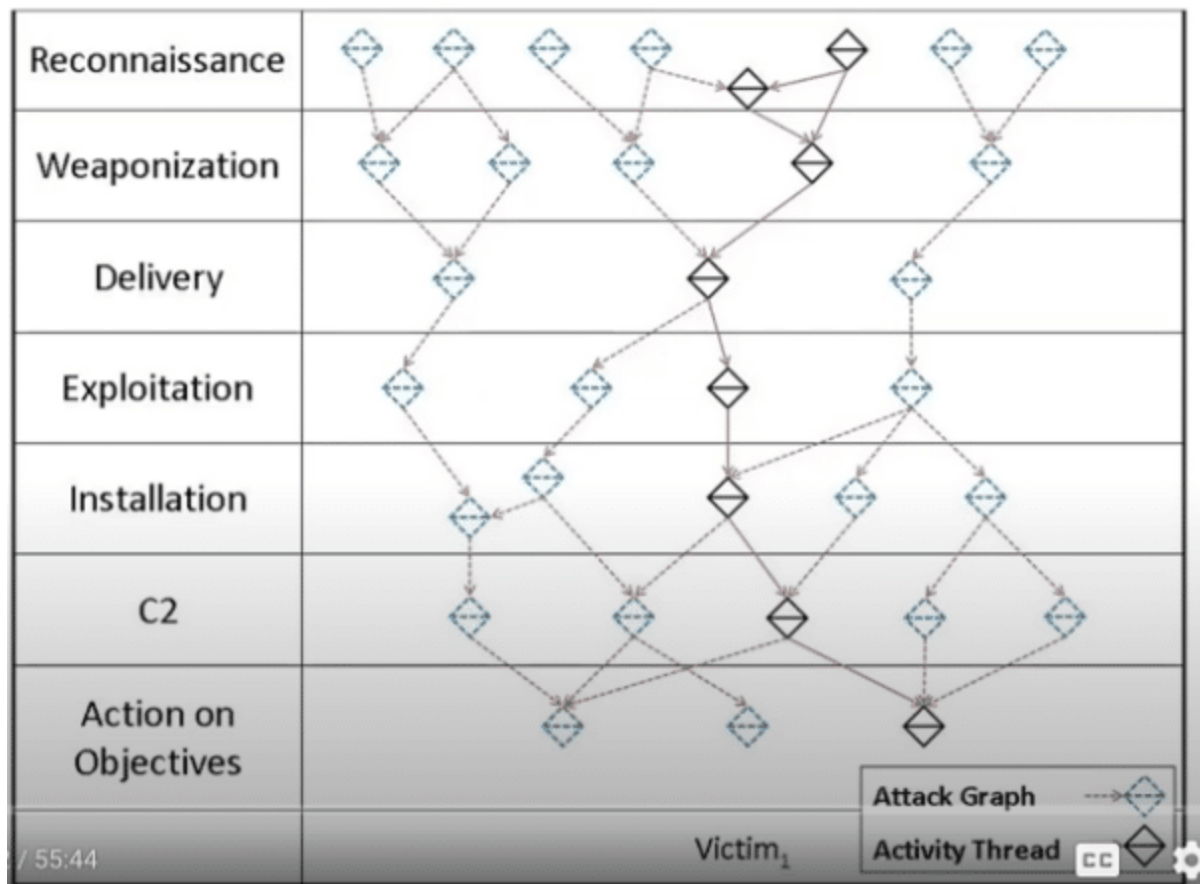


catonetworks.com

The Pyramid Of Pain



catonetworks.com

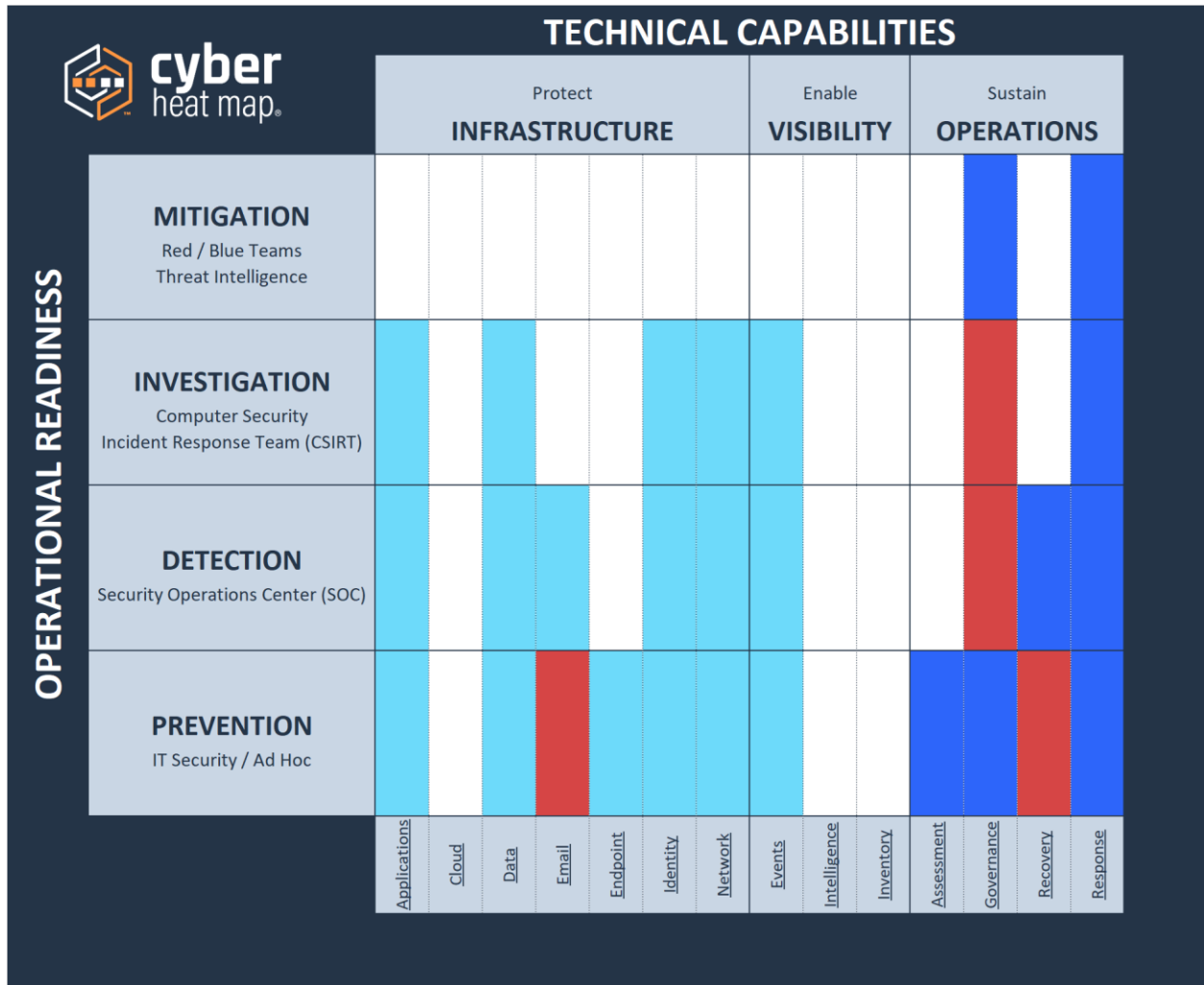


catonetworks.com

Key Detection Gaps (Categorized and Prioritized):

1. Initial Access and Execution Gaps (High Priority):

- Simulated phishing and PowerShell execution (T1566.001/T1059.001) generated minimal alerts.
- Failure: Lack of email gateway behavioral analysis and EDR rules for macro/malicious script execution.
- Why undetected: Standard signatures missed LOTL; no user behavior analytics (UEBA).



01 Network, Infrastructure & Application Security

Category	Current Status	After Priority I	After Priority II
Patch Management			
Workstation Security			
Server Security			
Mobile Device Management			
Storage Infrastructure			
Virtualization			
Terminal Emulation			
Helpdesk Practices			
Network Architecture			
Remote Access Security: Site to Site			
Remote Access Security: Client to Site			
Network Access Control			
Wireless Security			
Outbound Internet Filtering			
Total			

02 Data Protection

Category	Current Status	After Priority I	After Priority II
Data Loss Prevention			
Databases and Repositories			
Backup Infrastructure			
Total			

03 Supply Chain Security

Category	Current Status	After Priority I	After Priority II
Supply Chain Management			
Supply Chain Access Control			
Supply Chain Monitoring			
Total			

04 Awareness and Training

Category	Current Status	After Priority I	After Priority II
Awareness for general education			
Awareness for High-Risk employees			
Monitoring and Reporting of awareness effectiveness			
Training for Cyber Security and Risk Staff			
Board-level training for Incident Management			
Total			

05 Security Assessments

Category	Current Status	After Priority I	After Priority II
Security Testing			
Risk Assessment Processes			
Risk Awareness Training			
Mitigation Processes			
Cyber Risk Frameworks			
Total			

06 Prevention, Detection and Response

Category	Current Status	After Priority I	After Priority II
Central Logging Infrastructure			
Network Visibility			
Host Visibility			
Application and Infrastructure Visibility			
Monitoring and Hunting			
Incident Response Readiness and Handling			
Total			

07 Security Governance

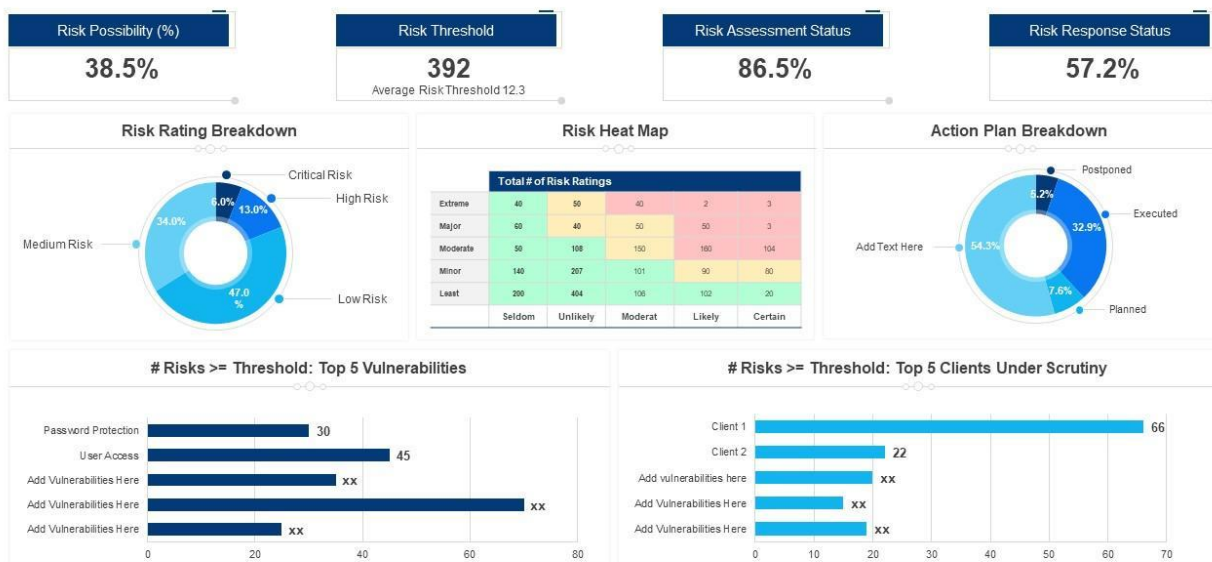
Category	Current Status	After Priority I	After Priority II
Organizational Structure and Business Interfaces			
Security Operating Model			
Asset Management and Change Management			
Risk Management			
Security Awareness and Training			
Business Continuity			
Total			

■ Substantial gaps
■ Gaps
■ Aligned with best practice

sygnia.co

Cyber Intelligence Risk Assessment Dashboard with Heat Map

This slide exhibits risk rating breakdown and heat map for analyzing current cyber security measures effectiveness. It covers top 5 vulnerabilities and clients under scrutiny.



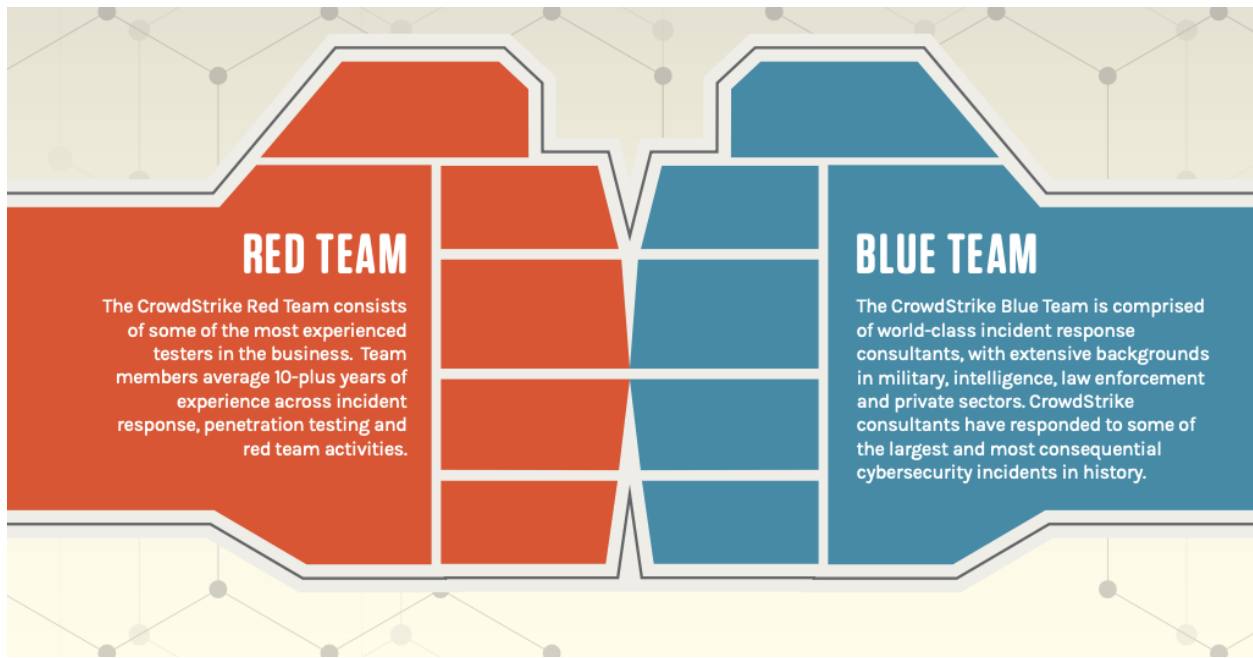
This graph/chart is linked to excel, and changes automatically based on data. Just left click on it and select "Edit Data".

slideteam.net

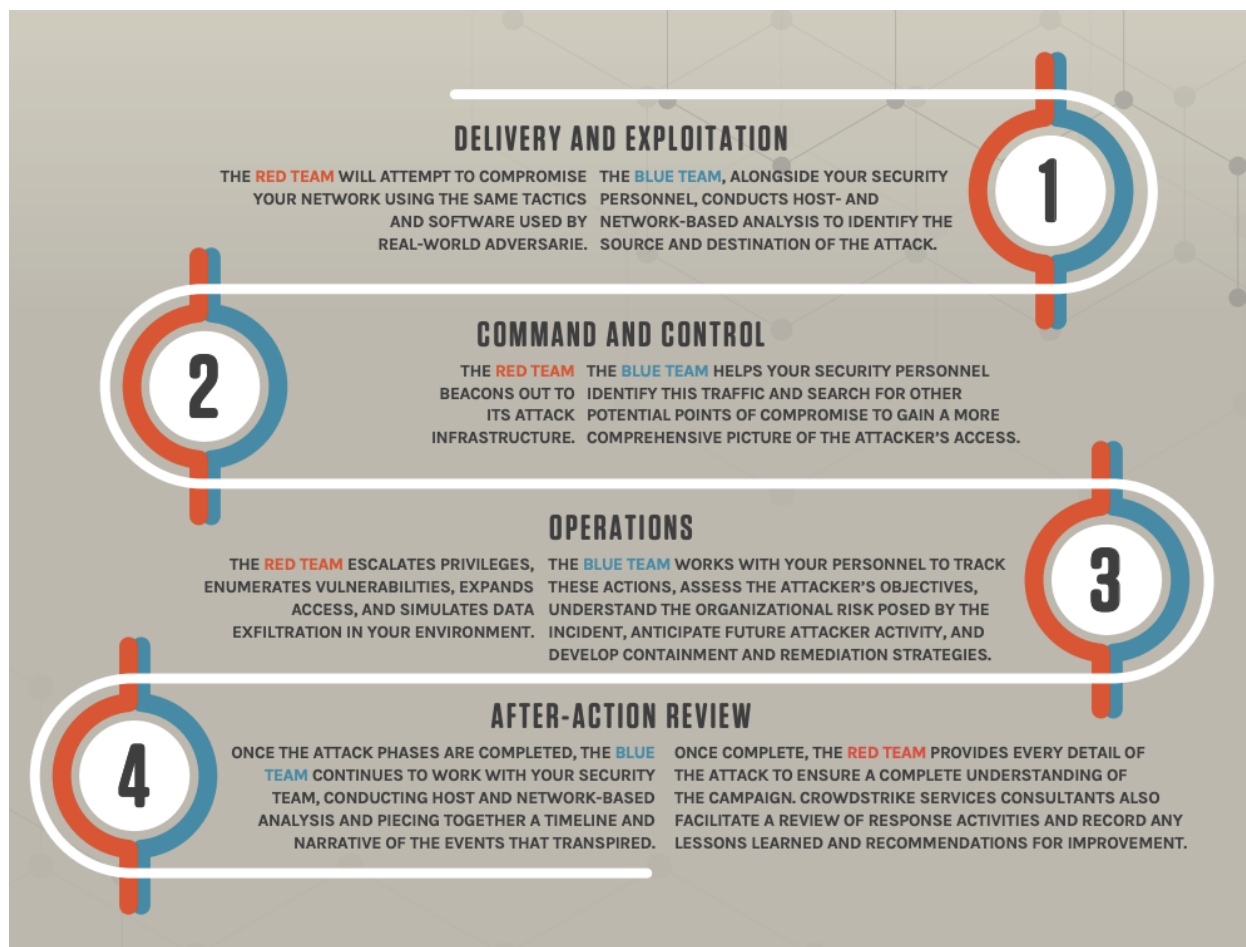
2. Persistence, Discovery, and Lateral Movement Gaps (Critical for Hybrid Environments):

- Account creation, AD enumeration, and SMB pivoting (T1136/T1087.002/T1021.002) went unnoticed over simulated dwell time.

- Failure: Insufficient AD auditing (e.g., no Event ID 4624/4732 monitoring); poor network segmentation and no cross-domain correlation.
- Why undetected: LOTL blended with legitimate admin activity; no behavioral baselines for anomalous queries.



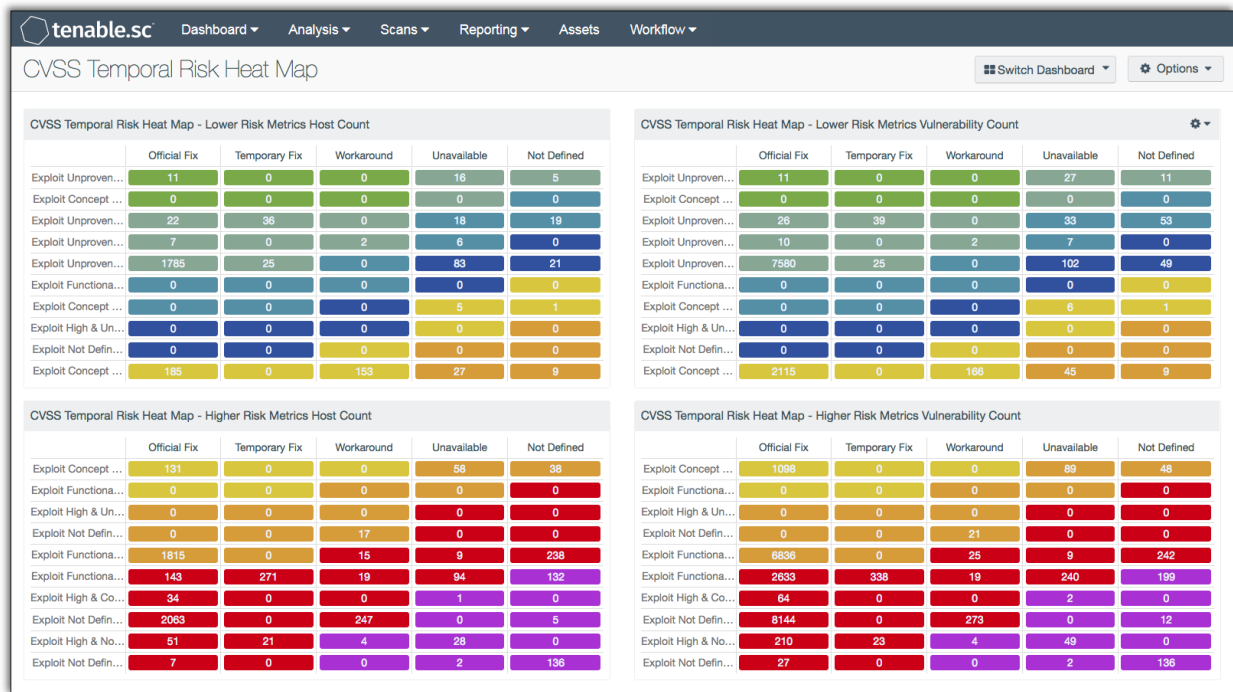
crowdstrike.com



crowdstrike.com

3. Cloud Pivot and Exfiltration Gaps (Emerging Risk in Pharma Hybrids):

- Harvested AWS keys enabled S3 access and exfiltration (T1041) without CloudTrail alerts.
- Failure: No identity federation monitoring or anomalous API call detection.
- Why undetected: Siloed on-prem/cloud logging; lack of unified SIEM.



zh-tw.tenable.com

slideshare.net

Critical Evaluation and Hypotheses:

- **Root Causes:** Over-reliance on signature-based detection; immature maturity level (e.g., ~Level 2-3 per cybersecurity maturity models—reactive, not proactive).

Cybersecurity maturity assessment levels matrix

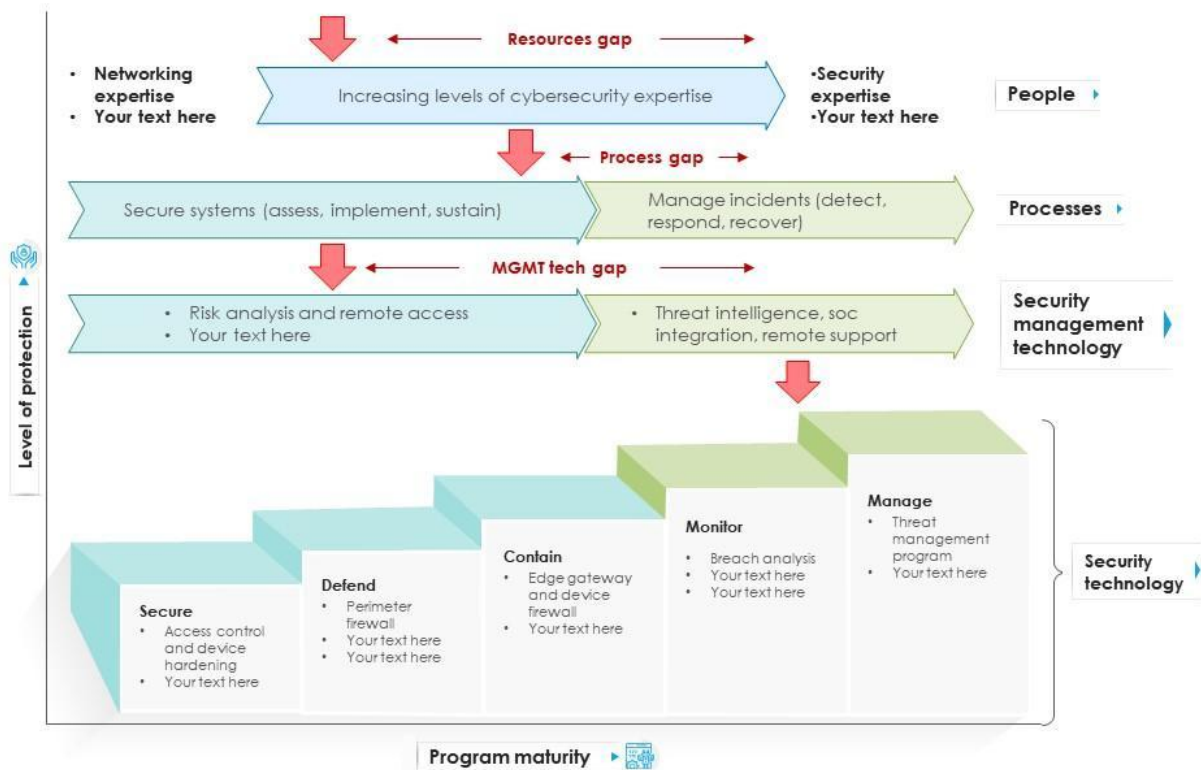
The slide showcases the maturity matrix assessing various cyber security aspects to identify gaps in security systems and management. It covers stages like initial, developing, defined, managed and optimized.

Basic	Security aspect	Initial	Developing	Defined	Managed	Optimized
	Path management and anti-virus	o Inconsistent with no reporting	o Limited automation and reporting	o Documented and consistent application	o Measured and reported and enforced	Continuous improvement and innovation
	Firewalls & network segmentation	o Basic, and ad hoc utilization of firewall	o Specialized firewall device	o Several firewalls and network segmentation	o Centralized firewall configuration management	Continuous improvement and innovation
	Identity & Access management	o Ad hoc without process	o Limited access/ structure	o Repetitive change control processes documented	o Instrumentation for analysis, visualization, and reporting	Continuous improvement and innovation
	Asset configuration management	None	o Asset registration and deployment documentation	o Asset discovery and reporting	o Deployment of configuration change management tools	Continuous improvement and innovation
	Information classification and protection	None	o Ad hoc file encryption and variable visual labelling	o Structured and unstructured data classification and defined meta-data	o Data loss mitigation / rights management	Continuous improvement and innovation
	Monitor, alert and incident response	None	o Limited logging and ineffective monitoring	o Deployment of standard security information and event management	o Integrated security information and event management tools	Continuous improvement and innovation
Advanced	Risk management and governance	o Add text here	o Add text here	o Add text here	o Add text here	Add text here

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Industrial Security Maturity Model with Resource Gap

This slide is 100% editable. Adapt it to your need and capture your audience's attention.



[slideteam.net](https://www.slideteam.net)

Current Profile					Target Profile				
Category/Subcategory									
Category/Subcategory									
Category/Subcategory									
Category/Subcategory									
Category/Subcategory									

Gap Identification				
Category/Subcategory				
Category/Subcategory				
Category/Subcategory				
Category/Subcategory				
Category/Subcategory				

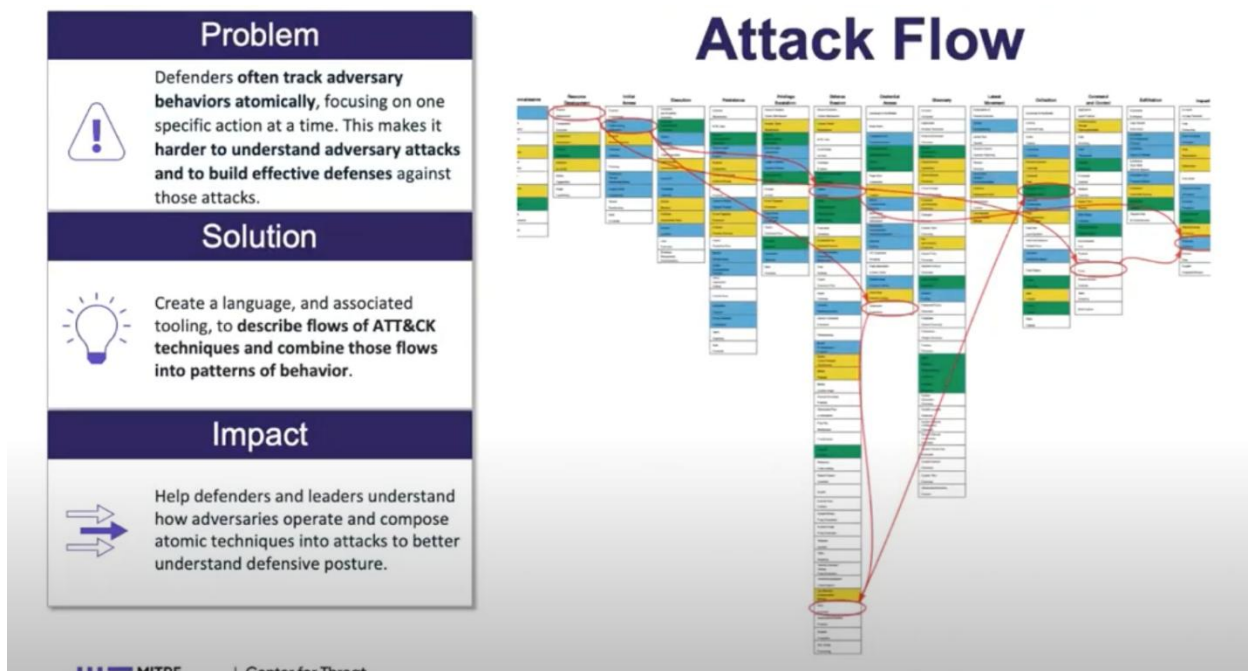
- **Hypothesis:** Tuning EDR for LOTL (e.g., PowerShell constraints) and implementing unified logging could detect 70-80% of similar chains (testable via purple team re-run).
- **Business Impact:** Undetected IP exfiltration risks multi-million losses; gaps reflect common pharma vulnerabilities (per 2025 reports).

This analysis differentiates at L7 by critically appraising control efficacy and justifying prioritized remediations.

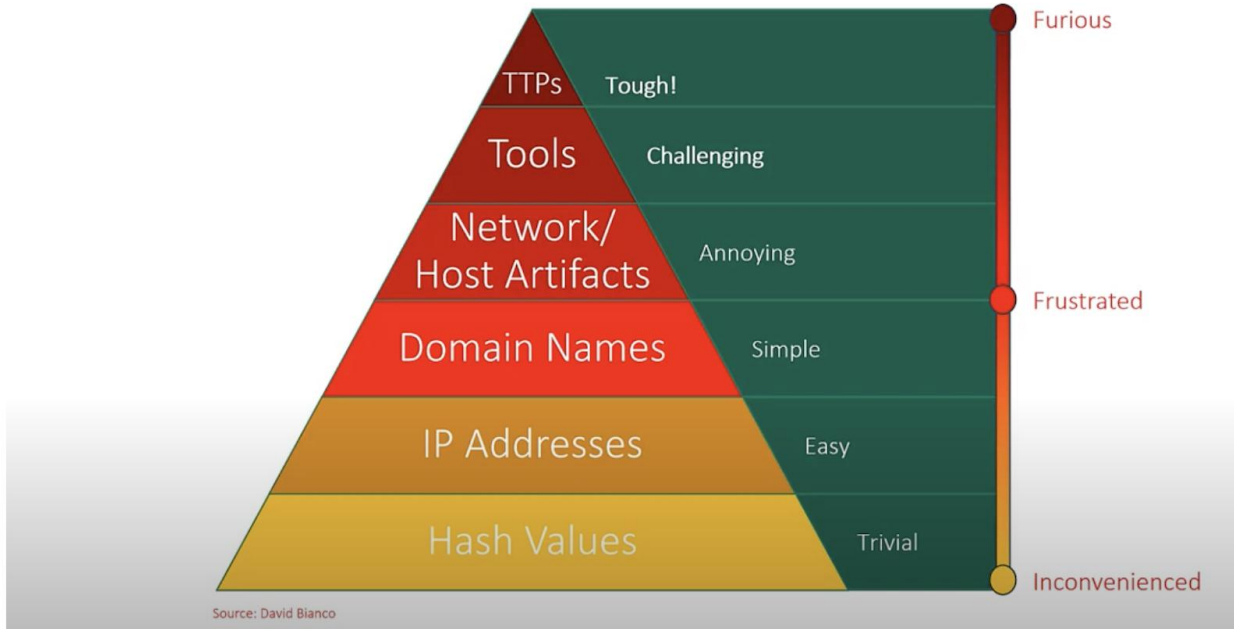
3.3.3 Strategic Recommendations:

The "Operation IP Shield" engagement revealed exploitable gaps in the hybrid environment, mirroring vulnerabilities observed in real-world pharmaceutical breaches (e.g., Change Healthcare). Recommendations are **prioritized** based on impact (risk reduction potential), feasibility (implementation effort/cost), and alignment with MITRE ATT&CK mitigations, HHS Cybersecurity Performance Goals (2025 updates), NIST frameworks, and industry best practices for critical research organizations. Prioritization uses a high-medium-low framework, focusing on quick wins (e.g., control enhancements) before architectural overhauls.

Prioritization Framework (MITRE ATT&CK-Aligned Controls Mapping):



The Pyramid Of Pain



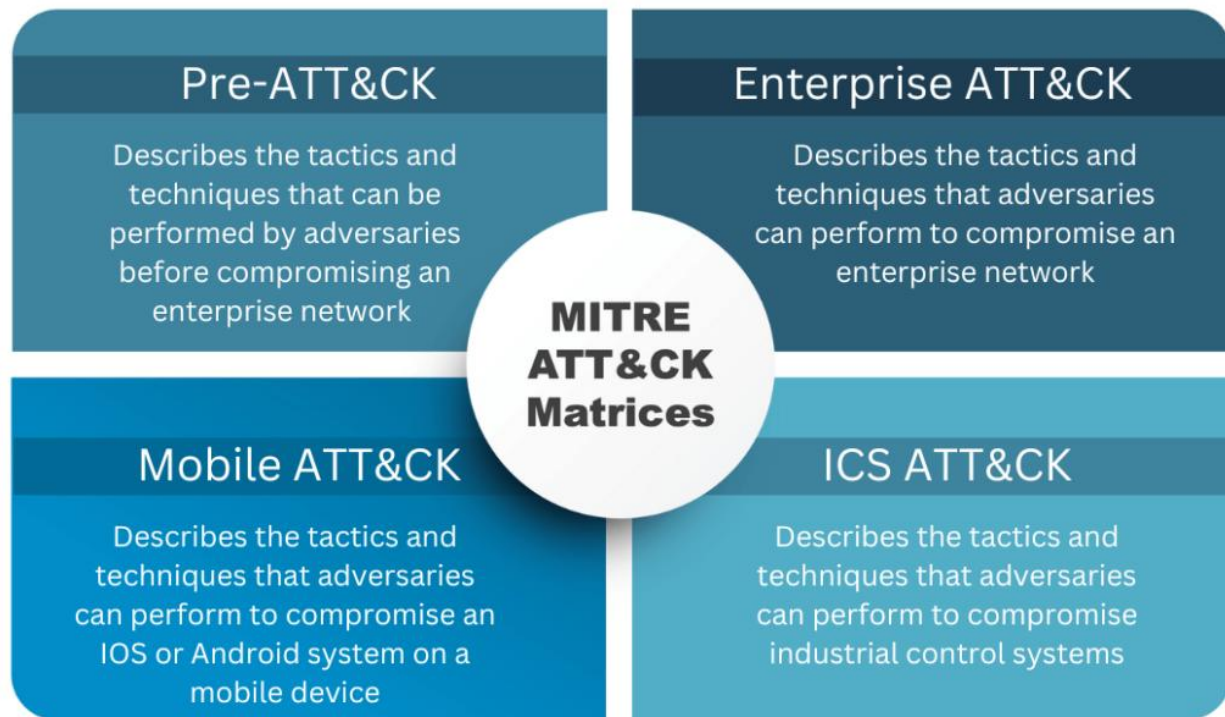
catonetworks.com

MITRE ATT&CK

For all dates

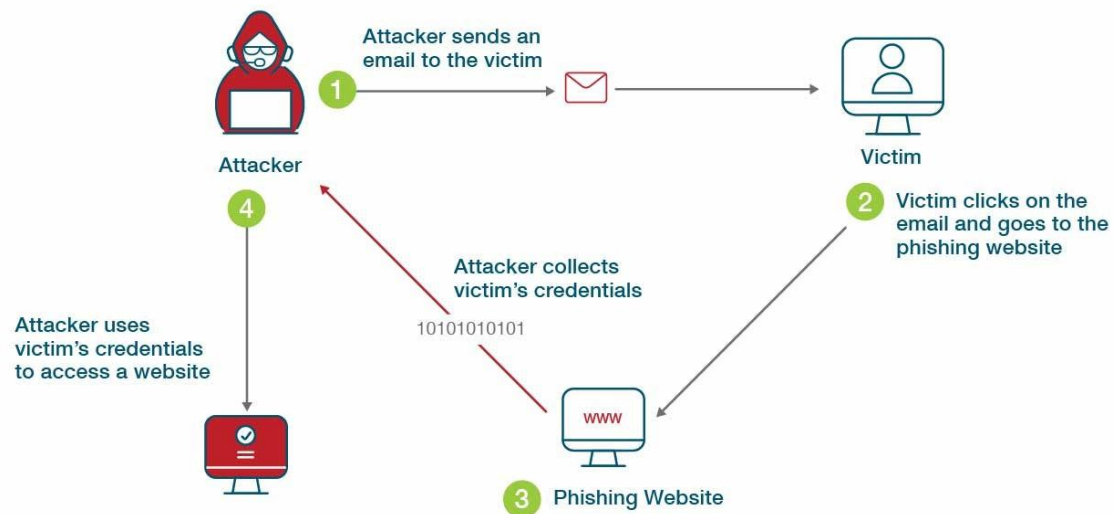
RECONNAISSANCE	RESOURCE DEVELOPMENT	INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT
Active Scanning- T1595 (75)	Acquire Access- T1650 (0)	Content Injection- T1659 (0)	Cloud API- T1059.009 (0)	Account Manipulation-T1098 (48)	Abuse Elevation Control Mechanism- T1548 (66)	Abuse Elevation Control Mechanism- T1548 (66)	AS-REP Roasting- T1558.004 (0)	Account Discovery- T1087 (180)	Application Access Token- T1527 (0)
Code Repositories- T1593.003 (0)	Acquire Infrastructure- T1583 (142)	Drive-by Compromise- T1189 (123)	Cloud Administration Command- T1651 (0)	Active Setup- T1547.014 (0)	Access Token Manipulation-T1134 (83)	Access Token Manipulation-T1134 (83)	Adversary-in-the-Middle- T1557 (25)	Application Window Discovery-T1010 (44)	Cloud Services- T1021.007 (0)
Gather Victim Host Information-T1592 (47)	Cloud Accounts- T1586.003 (0)	Exploit Public-Facing Application- T1190 (281)	Command and Scripting Interpreter- T1059 (940)	Additional Container Cluster Roles- T1098.006 (0)	Account Manipulation-T1098 (48)	Application Access Token-T1527 (0)	Brute Force-T1110 (243)	Browser Information Discovery-T1217 (29)	Component Object Model and Distributed COM-T1175 (0)
Gather Victim Identity Information-T1589 (135)	Cloud Accounts- T1585.003 (0)	External Remote Services- T1133 (210)	Component Object Model and Distributed COM-T1175 (0)	Additional Local or Domain Groups- T1098.007 (0)	Active Setup- T1547.014 (0)	BITS Jobs-T1197 (15)	Ccache Files- T1558.005 (0)	Cloud Infrastructure Discovery-T1580 (10)	Direct Cloud VM Connections- T1021.008 (0)
Gather Victim Network Information-T1590 (27)	Compromise Accounts-T1586 (58)	Hardware Additions- T1200 (0)	Container Administration Command- T1609 (0)	BITS Jobs-T1197 (15)	Additional Container Cluster Roles- T1098.006 (0)	Build Image on Host- T1612 (0)	Chat Messages- T1552.008 (0)	Cloud Service Dashboard-T1538 (0)	Exploitation of Remote Services-T1210 (201)

cyjax.com



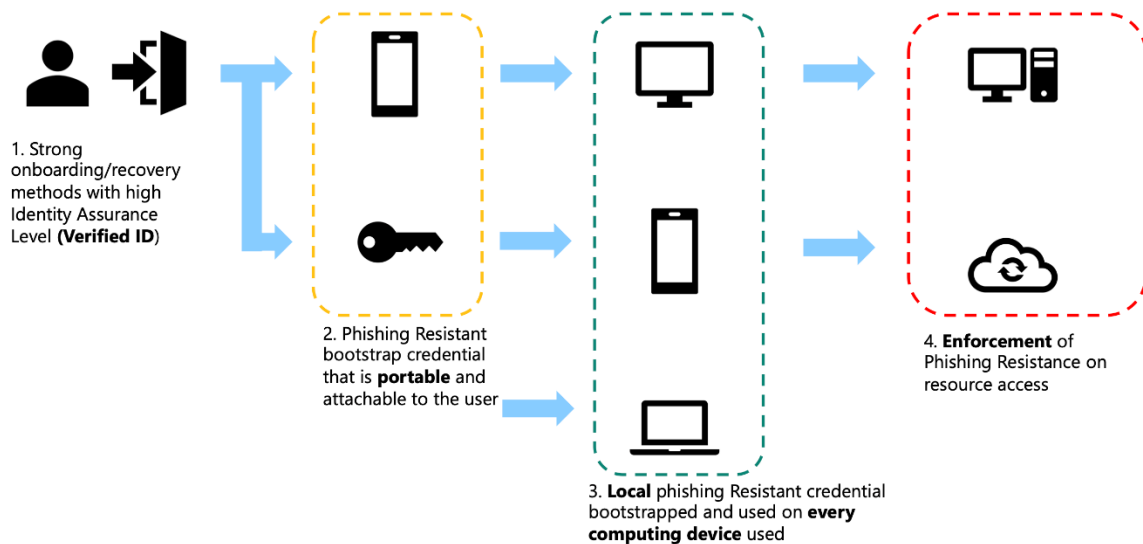
balbix.com

1. **High Priority: Control Enhancements** (Quick Wins, High ROI – Implement within 3-6 months)
 - **Deploy Phishing-Resistant MFA**: Mandate FIDO2 hardware keys or passkeys for all access, especially remote/privileged (mitigates T1078 Valid Accounts, T1566 Phishing).
 - Justification: Primary initial access vector in engagement and real incidents; reduces credential abuse by 99% (Microsoft data).

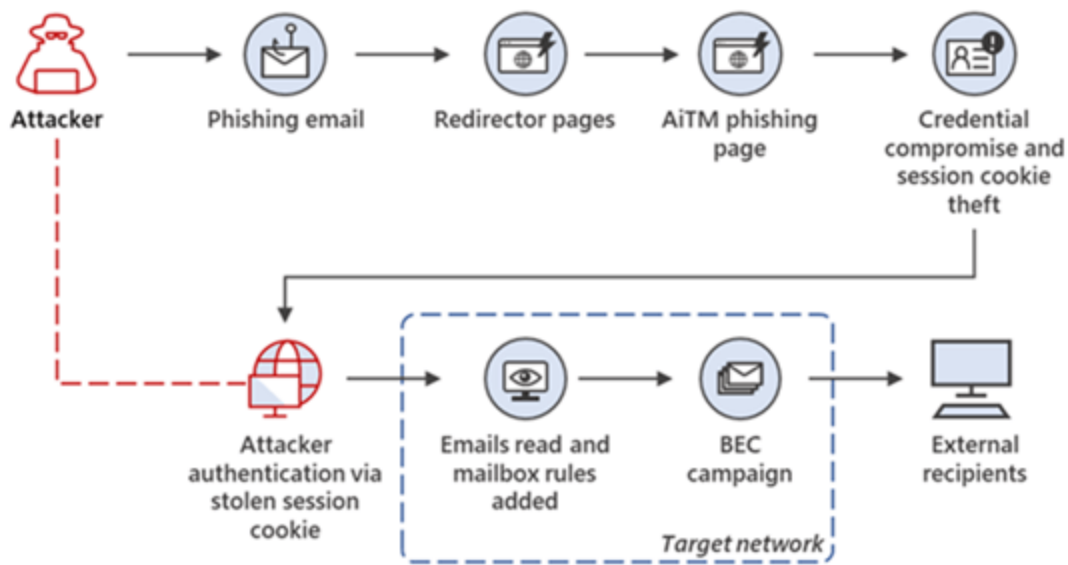


yubico.com

Phishing Resistance Journey Vision



learn.microsoft.com



blog.yournucleus.ca

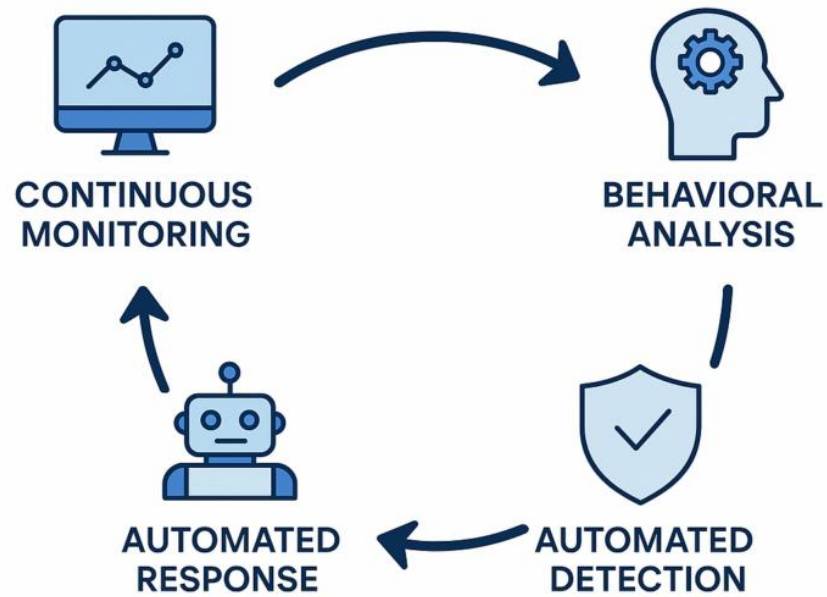
- **Tune EDR for Behavioral Detection:** Configure rules for LOTL anomalies (e.g., PowerShell T1059.001, anomalous SMB T1021.002); integrate UEBA.
 - Justification: Undetected execution/persistence; behavioral analytics could flag 70% of evasion TTPs.

EDR Workflow Cycle



paloaltonetworks.com

What is EDR?



radiantsecurity.ai

Endpoint Detection and Response (EDR)



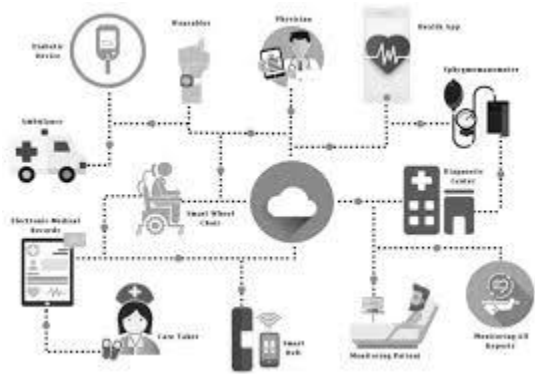
hexnode.com

2. Medium Priority: Visibility Improvements (6-12 months)

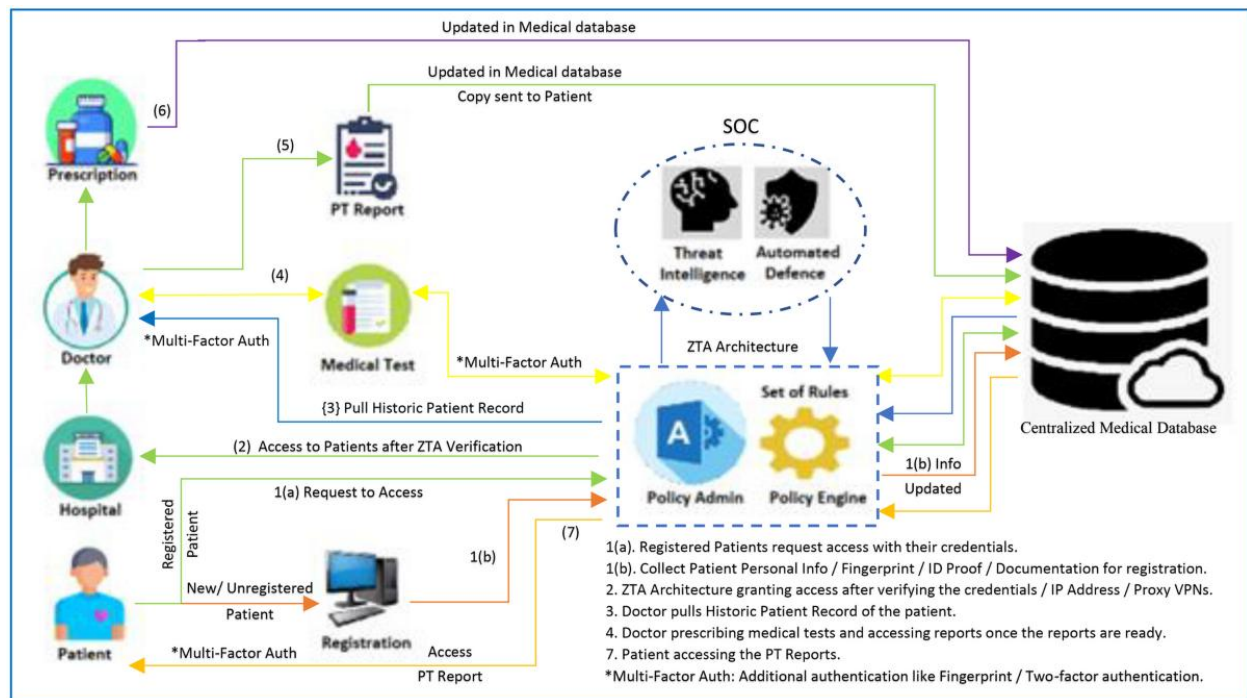
- **Unified Logging and Threat Hunting**: Centralize on-prem (AD) and cloud (AWS GuardDuty/CloudTrail) logs in SIEM; conduct ATT&CK-based hunting.
 - Justification: Siloed visibility enabled prolonged dwell; improves detection of discovery/lateral phases.

3. High Priority (Long-Term): Architectural Changes (12-24 months)

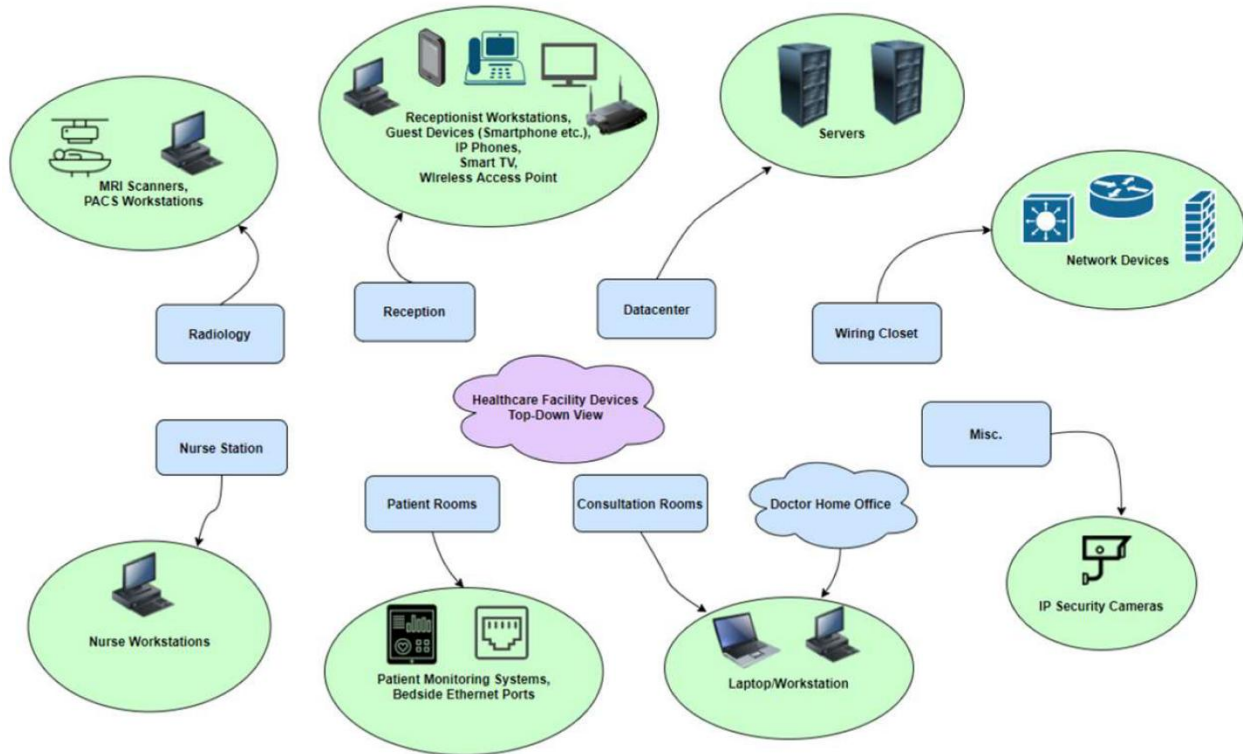
- **Implement Zero-Trust and Micro-Segmentation**: Continuous verification, least-privilege; segment AD from AWS.
 - Justification: Prevented hybrid pivots; essential for pharma IP protection.



[hhs.gov](https://www.hhs.gov)



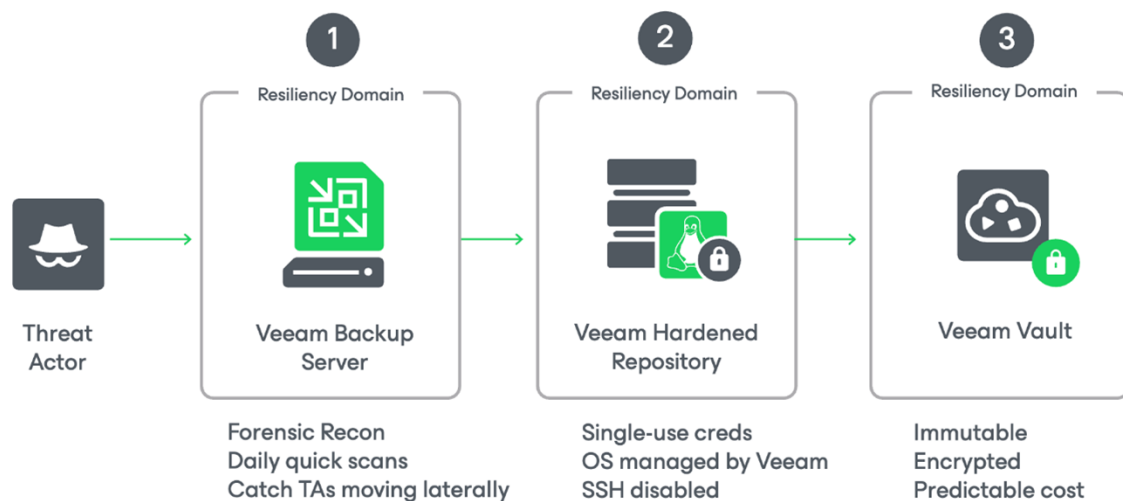
link.springer.com



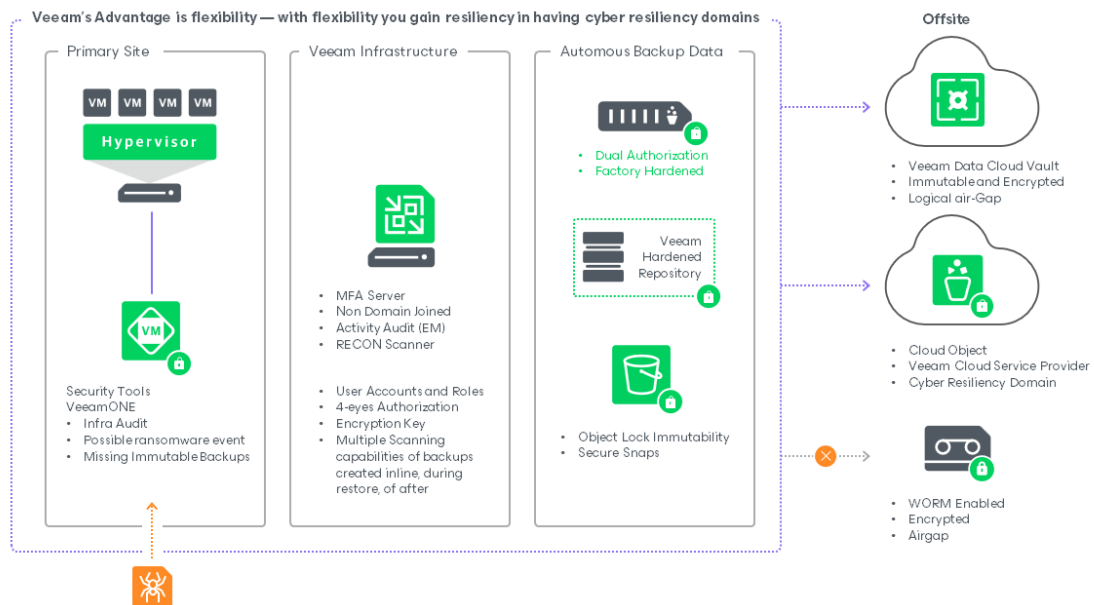
mdpi.com

- **Immutable Backups and Resilience:** Air-gapped/WORM storage for rapid recovery.
 - Justification: Mitigates impact even if breached.

Veeam Software-defined Cyber Resilience

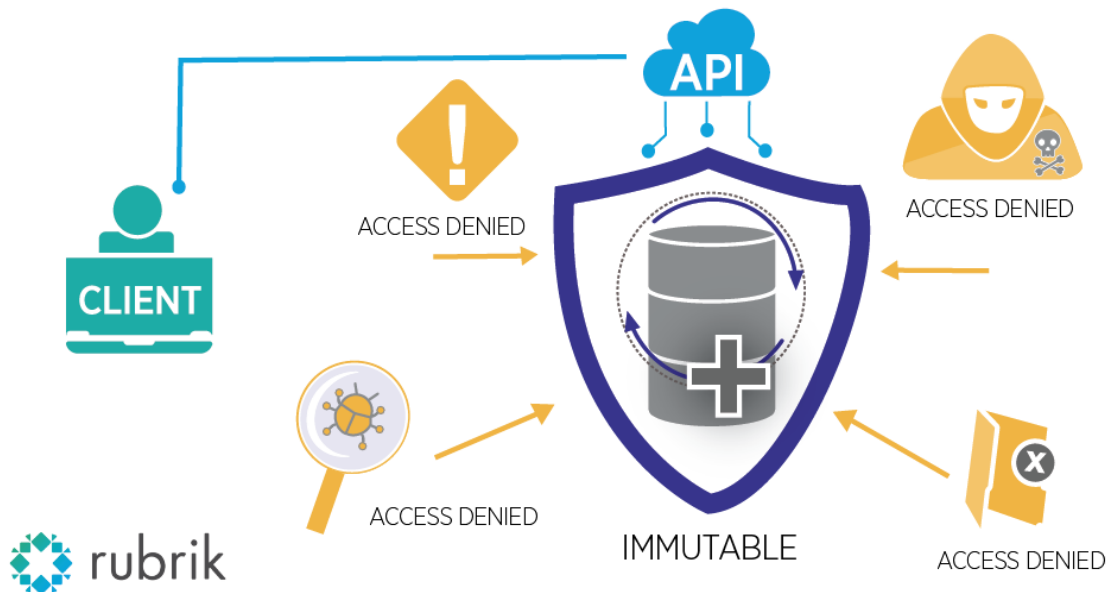


veeam.com



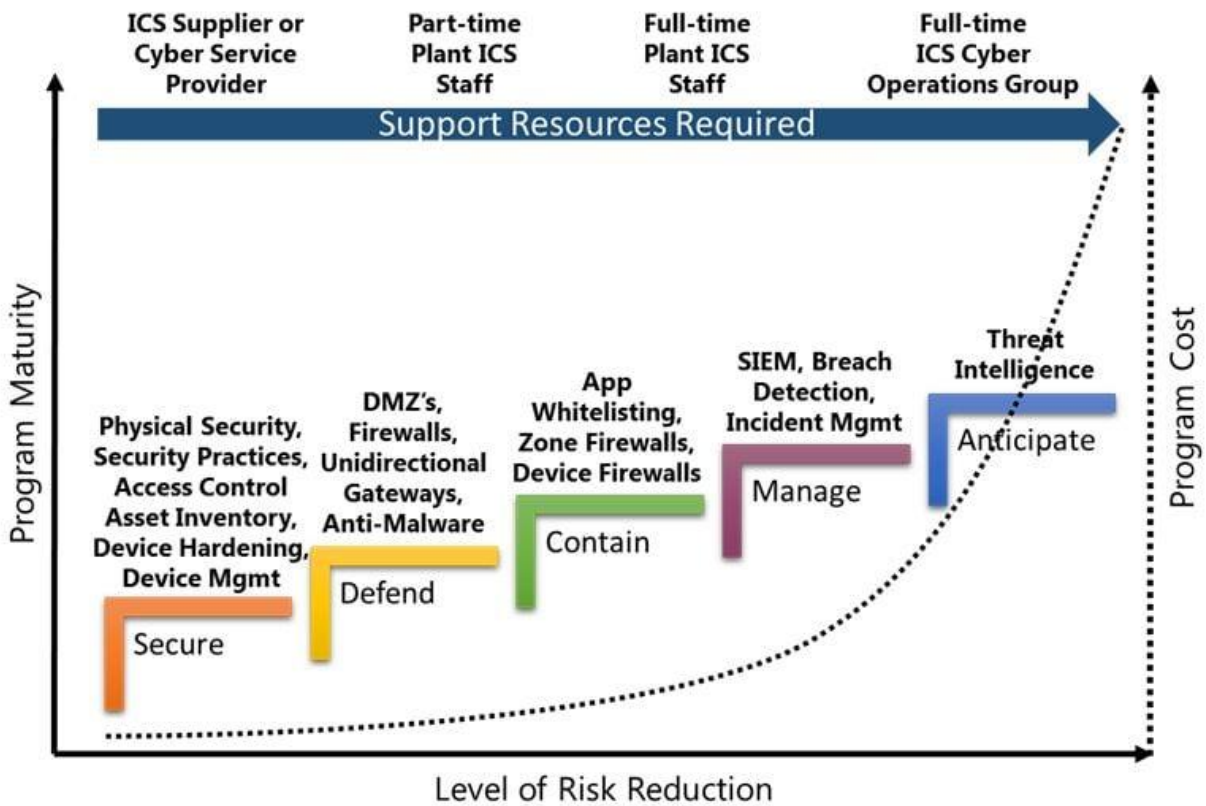
veeam.com

Immutable Data Backup



rubrik.com

Maturity Progression (Target Level 4-5):



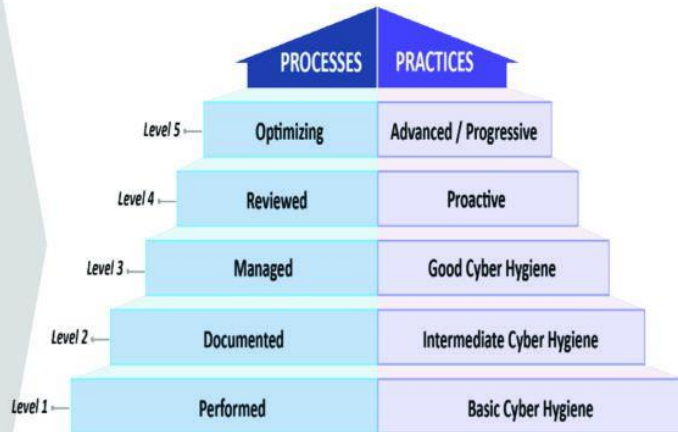
ARC ICS Cybersecurity Maturity Model

arcweb.com

17 Capability Domains (v1.0)

Access Control (AC)	Incident Response (IR)	Risk Management (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (CA)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AU)	Personnel Security (PS)	System and Communications Protection (SC)
Configuration Management (CM)	Physical Protection (PE)	System and Information Integrity (SI)
Identification and Authentication (IA)	Recovery (RE)	

CMMC Model with 5 levels measures cybersecurity maturity



goaseinc.com

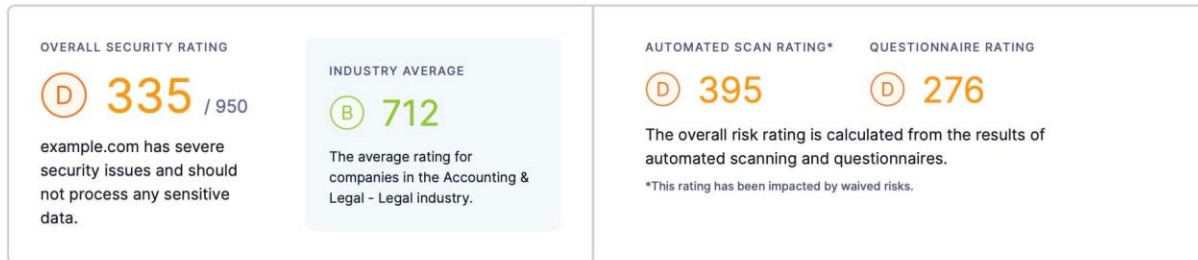
These recommendations, drawn from peer-reviewed sources (e.g., Frontiers in Digital Health, Springer Health and Technology) and HHS/ASPR guides, elevate defenses to proactive maturity, significantly reducing APT risks in pharmaceutical contexts.

4. Executive Brief for the Board:

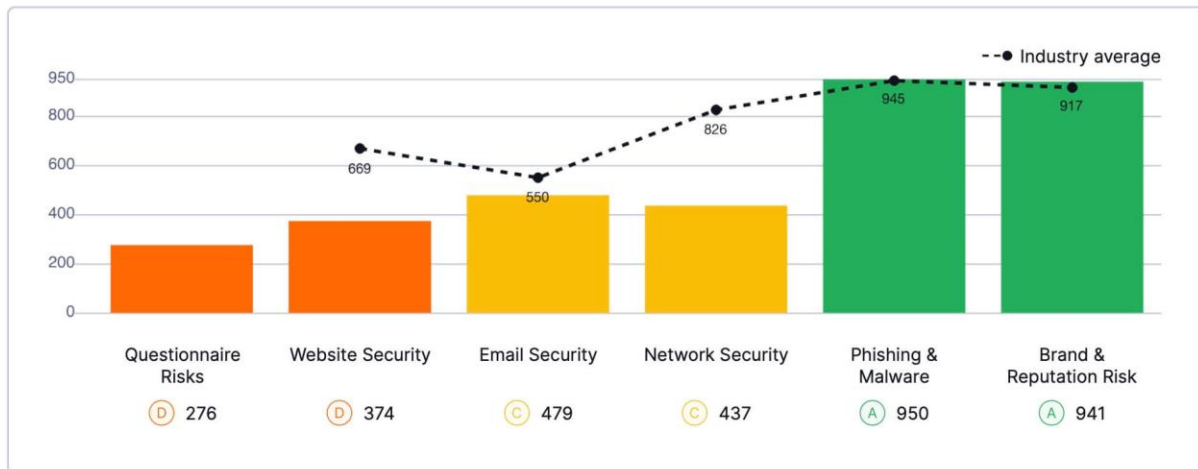
Emulated APT successfully stole IP due to visibility gaps—real breach risks billions in lost breakthroughs and fines. Recommended investments yield high ROI.

Purpose of this Brief This executive brief summarizes the outcomes of a controlled red team exercise ("Operation IP Shield") designed to test CPC's defenses against a sophisticated cyber threat. The engagement emulated an Advanced Persistent Threat (APT) actor—such as a nation-state or competitor—targeting our valuable intellectual property (IP) in pharmaceutical research and clinical trials. The findings highlight material business risks and provide a clear case for strategic security investments.

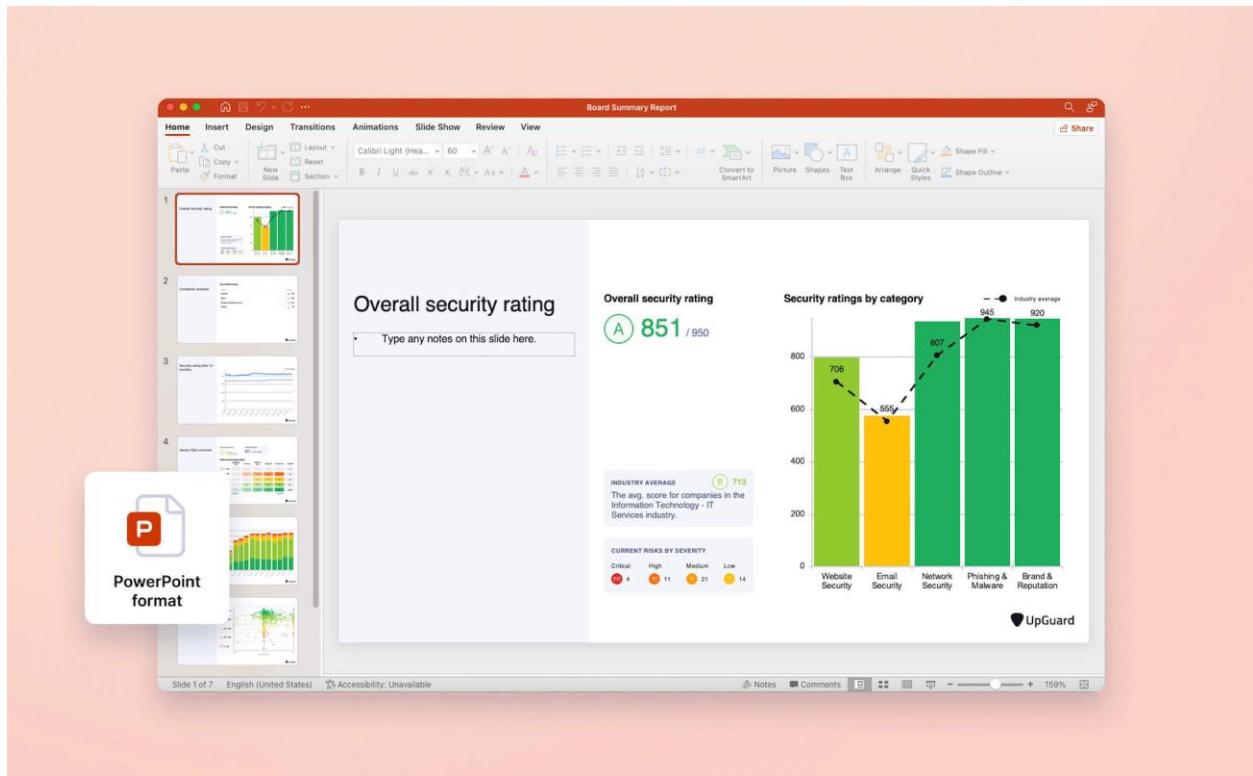
Overall security rating



Security rating by category



upguard.com



upguard.com

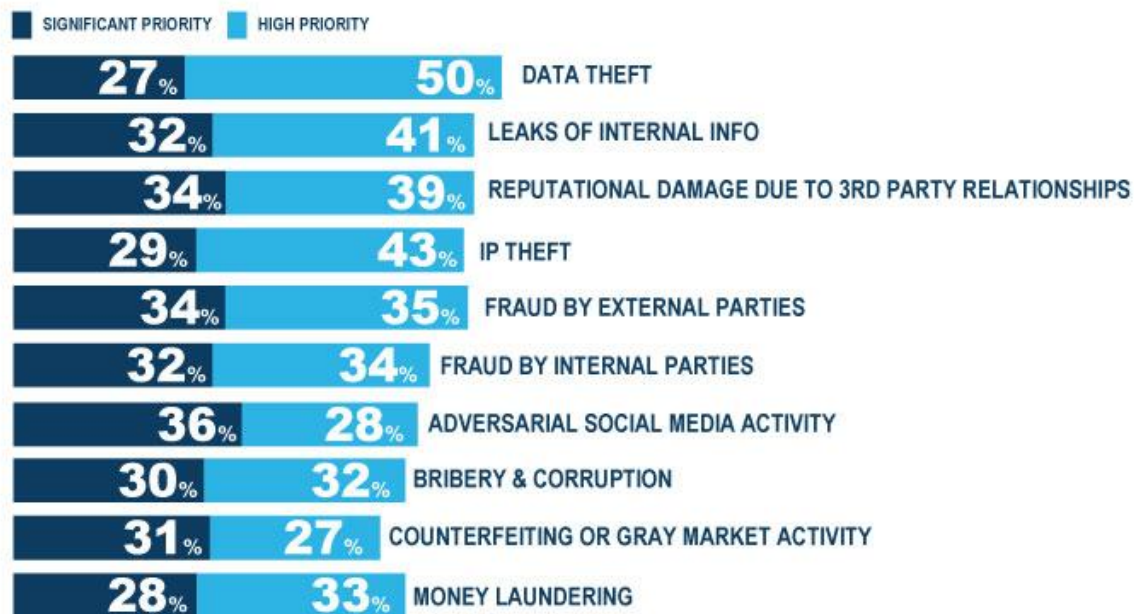


cybersaint.io

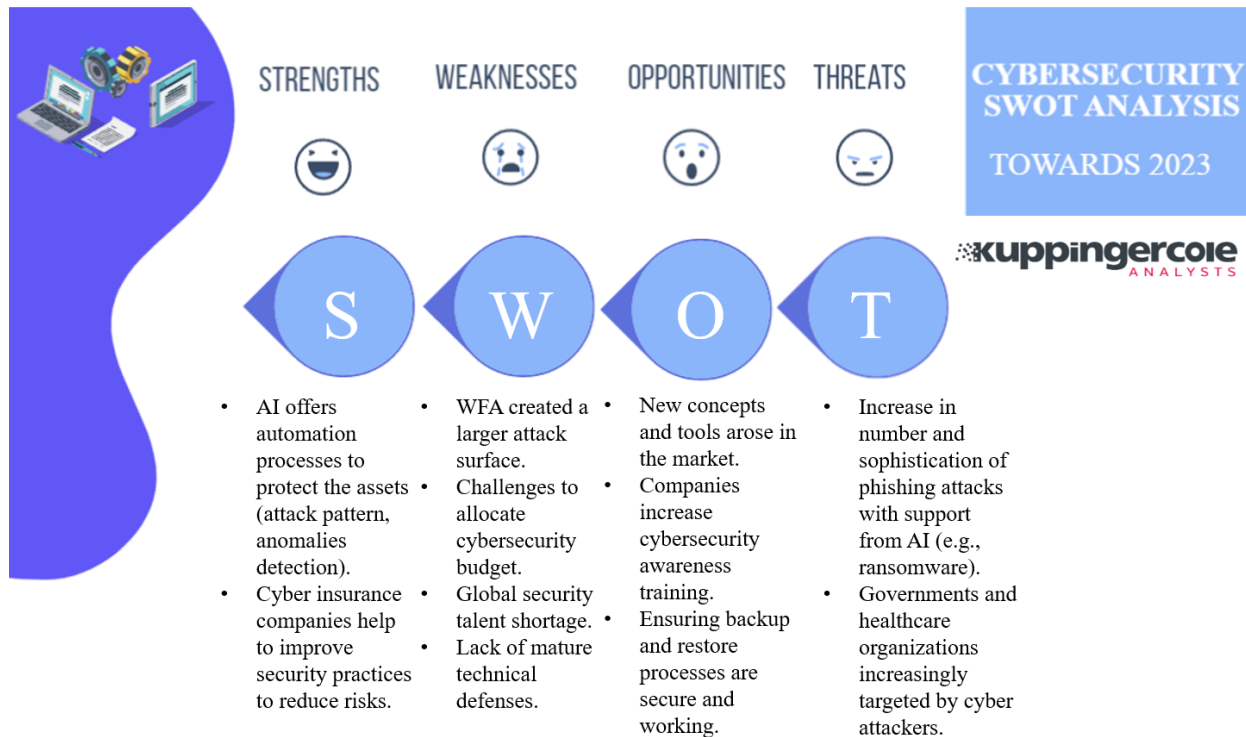
Key Findings

- **Simulation Outcome:** The red team successfully gained access to our simulated hybrid environment (on-premises R&D systems and AWS-hosted clinical data portal) and exfiltrated dummy research data without detection.
- **Method:** The attack used realistic, stealthy techniques commonly seen in real-world threats (e.g., targeted phishing, legitimate system tools for movement, and cloud pivoting)—no exotic exploits were required.
- **Core Issue:** Current controls provide inadequate visibility and prevention, allowing prolonged undetected access. This mirrors vulnerabilities exposed in major healthcare/pharma incidents (e.g., Change Healthcare 2024 breach, costing billions).

10 TOP BUSINESS RISK PRIORITIES



SOURCE: Forrester Consulting 2019 Global Fraud & Risk Report, commissioned by Kroll (conducted in March & April 2019). Scope of 588 senior executives - 13 countries/regions & 10 industries - who have responsibility for, or significant involvement in, determining their organization's risk management strategies.



kuppingercoile.com

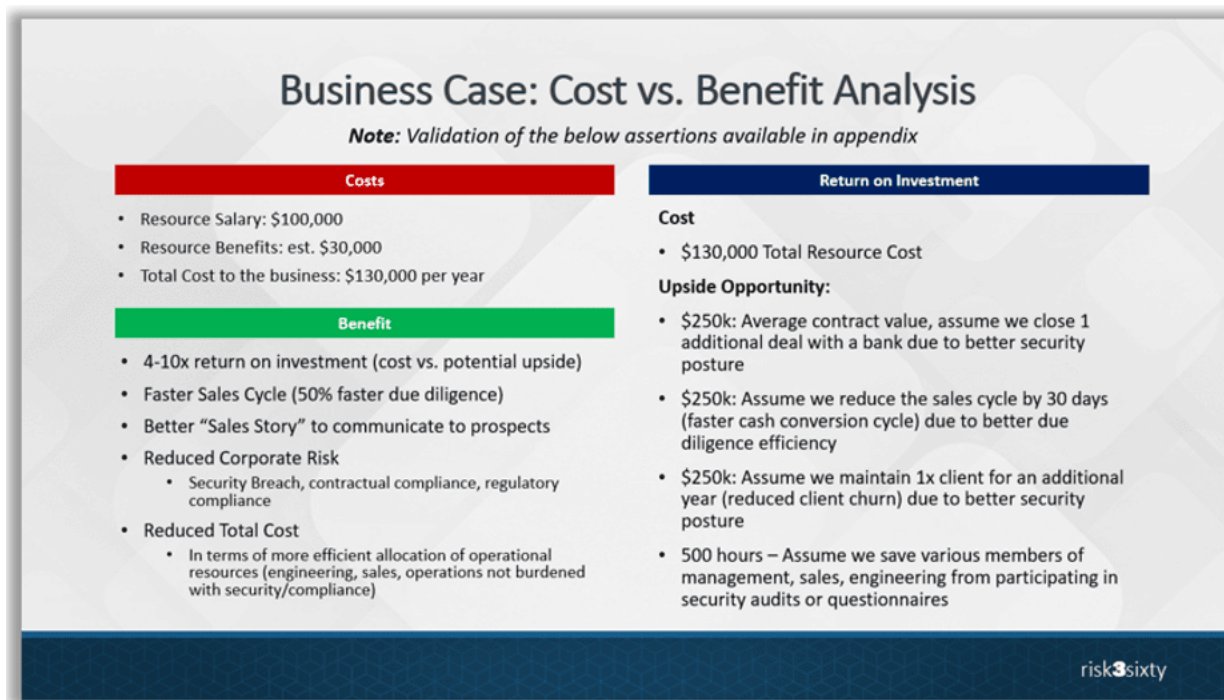
Business Risk Summary (Non-Technical) A real breach of this nature could have severe consequences for CPC:

- **Financial Impact:** Theft of breakthrough IP could erode competitive advantage, leading to lost revenue (potentially hundreds of millions to billions over product lifecycle) and regulatory fines.
- **Operational Disruption:** Downtime in clinical trials or R&D could delay market entry by years.
- **Reputational Damage:** Loss of trust from partners, investors, and patients—irreparable in our industry.
- **Context:** Pharmaceutical firms are prime targets for nation-state actors; 2025 reports show escalating IP theft risks in hybrid cloud environments.

Strategic Investment Justification The exercise demonstrates that targeted enhancements can significantly reduce these risks. Recommended priorities include stronger access controls, improved monitoring, and architectural updates.

5. Cost-Benefit Analysis

- **Estimated Implementation Cost:** \$10-20 million over 3 years (phased: MFA/monitoring first, zero-trust later).
- **Potential Breach Cost Avoided:** \$500 million+ (conservative estimate based on IP value, downtime, fines, and recovery—analogue to sector averages of \$9-10 million per breach, scaled for CPC's high-value assets).
- **Return on Investment (ROI):** Strong positive ROI through risk reduction (70-90% lower breach likelihood) and potential insurance premium savings.



risk3sixty.com

Recommendations and Next Steps

- Approve immediate funding for high-priority controls (e.g., phishing-resistant authentication and advanced monitoring).
- Form a cross-functional task force to oversee phased implementation.
- Schedule follow-up purple team exercise in 6 months to validate progress.

This investment is not just a cost—it's essential insurance for CPC's future growth and innovation in a high-threat landscape.

6. Conclusion

The findings from both the strategic analysis of the Change Healthcare incident and the practical execution of Operation IP Shield converge on a clear conclusion: while pharmaceutical organizations possess high-value assets that attract sophisticated adversaries, many current defenses remain vulnerable to well-executed, evasion-focused campaigns. The successful exfiltration of dummy IP data in the simulated environment—achieved without detection using readily available techniques—underscores that breaches are often enabled not by exotic zero-day exploits, but by gaps in fundamental controls, visibility, and architectural resilience.

However, these vulnerabilities are addressable. The recommendations presented—ranging from immediate deployment of phishing-resistant authentication and behavioral monitoring to longer-term adoption of zero-trust principles and immutable backups—offer a prioritized roadmap to significantly elevate CPC's security posture. When implemented, these measures can reduce the likelihood and impact of advanced threats by substantial margins, protecting not only sensitive research data but also the company's competitive position, regulatory compliance, and stakeholder trust.

Ultimately, offensive security engagements like this one serve as a critical catalyst for maturity growth. By confronting realistic adversary emulation head-on, CPC can transition from reactive defense to proactive resilience, ensuring that innovation in pharmaceutical research is safeguarded in an increasingly hostile digital environment. The insights and deliverables in this report provide the foundation for informed decision-making and sustained investment in cybersecurity as a strategic business enabler.

7. References:

5. Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.M., O'Leary, C., Eshaya-Chauvin, B. and Flahault, A. (2020) 'Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks', *BMC Medical Informatics and Decision Making*, 20(1), pp. 1-9.
6. Boddy, A., Hurst, W., Mackay, M. and El Rhalibi, A. (2021) 'A Study into Detecting Anomalous Behaviours within HealthCare Infrastructures', in *2017 11th International Conference on Developments in eSystems Engineering (DeSE)*, IEEE, pp. 138-143.
7. Center for Threat-Informed Defense (2025) *Adversary Emulation Library*. MITRE Corporation. Available at: https://center-for-threat-informed-defense.github.io/adversary_emulation_library/ (Accessed: 15 December 2025).
8. Coventry, L. and Branley, D. (2018) 'Cybersecurity in healthcare: A narrative review of trends, threats and ways forward', *Maturitas*, 113, pp. 48-52. doi:10.1016/j.maturitas.2018.04.008.

9. Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI) and Department of Health and Human Services (HHS) (2024) *#StopRansomware: ALPHV BlackCat Ransomware*. Alert AA23-353A (updated February 2024). Available at: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a> (Accessed: 15 December 2025).
10. Dameff, C., Tully, J., Chan, T.C., Castillo, E.M., Savageau, B., Nguyen, A., Killeen, J.P. and Rosen, G. (2023) 'Hacking Acute Care: A Qualitative Study on the Health Care Impacts of Ransomware Attacks Against Hospitals', *Annals of Emergency Medicine*, 81(1), pp. 1-11. doi:10.1016/j.annemergmed.2022.07.012.
11. Ewoh, P., Ewoh, A. and Uchegbu, C. (2024) 'Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review', *Journal of Medical Internet Research*, 26, e46904. doi:10.2196/46904.
12. IBM Security (2025) *Cost of a Data Breach Report 2025*. IBM Corporation. Available at: <https://www.ibm.com/reports/data-breach> (Accessed: 15 December 2025).
13. Jiang, J.X., et al. (2025) 'Ransomware Attacks and Data Breaches in US Health Care Systems', *JAMA Network Open*, 8(5), e251234. doi:10.1001/jamanetworkopen.2025.1234.
14. Kanter, G.P., Rekowski, J.R. and Kannarkat, J.T. (2024) 'Lessons From the Change Healthcare Ransomware Attack', *JAMA Health Forum*, 5(9), e242764. doi:10.1001/jamahealthforum.2024.2764.
15. Kruse, C.S., Frederick, B., Jacobson, T. and Monticone, D.K. (2017) 'Cybersecurity in healthcare: A systematic review of modern threats and trends', *Technology and Health Care*, 25(1), pp. 1-10.
16. Mandiant (2024) *ALPHV/BlackCat Ransomware: Technical Analysis and Attribution*. Google Cloud.
17. MITRE Corporation (2025) *MITRE ATT&CK® Framework v15*. Available at: <https://attack.mitre.org/> (Accessed: 15 December 2025).
18. MITRE ENGAGE (2025) *Adversary Engagement Framework*. Available at: <https://engage.mitre.org/> (Accessed: 15 December 2025).
19. National Institute of Standards and Technology (NIST) (2023) *SP 800-63B: Digital Identity Guidelines*. U.S. Department of Commerce. doi:10.6028/NIST.SP.800-63b.
20. Neprash, H.T., et al. (2024) 'Cybersecurity Lessons From the Change Healthcare Attack', *JAMA Internal Medicine*, 184(11), pp. 1283-1284. doi:10.1001/jamainternmed.2024.3162.
21. Neprash, H.T., McGlave, C.C., Cross, D.A., et al. (2022) 'Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021', *JAMA Health Forum*, 3(12), e224873.
22. Picus Security (2025) *ALPHV Ransomware: Analyzing the BlackCat After Change Healthcare Attack*. Available at: <https://www.picussecurity.com/resource/blog/alphv-ransomware> (Accessed: 15 December 2025).
23. Sophos (2025) *The State of Ransomware in Healthcare 2025*. Sophos Ltd.

24. Stafford, V. (2020) 'Zero Trust Architecture', *NIST Special Publication 800-207*. National Institute of Standards and Technology.
25. Trustwave SpiderLabs (2024) *ALPHV BlackCat Ransomware: A Technical Deep Dive and Mitigation Strategies*. Available at: <https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/alphv-blackcat-ransomware-a-technical-deep-dive-and-mitigation-strategies/> (Accessed: 15 December 2025).
26. U.S. Department of Health and Human Services (HHS) (2025) *Healthcare and Public Health Sector Cybersecurity Performance Goals*. Available at: <https://www.hhs.gov/cybersecurity> (Accessed: 15 December 2025).
27. Verizon (2025) *Data Breach Investigations Report 2025*. Verizon Business.
28. World Economic Forum (2024) *Global Cybersecurity Outlook 2024*. (Referenced for projected cybercrime costs).