XM Cyber

The Remedy Against Healthcare Attacks

3 Real-Life Attack Paths Shut Down By XM Cyber

In Healthcare, security hygiene is often high, yet the environment remains fragile. Perimeter defenses and "checked boxes" don't stop attackers. All these measures do is send them looking for detours. True resilience requires visibility into how seemingly minor exposures interconnect to create a direct line to your critical assets. Here are three real-world attack paths the XM Cyber Continuous Exposure Management platform identified and eliminated before attackers could leverage them.

The Healthcare Provider with the Compromised Download Folder

We often secure the front door (the perimeter) while leaving the internal "keys" sitting on the kitchen counter. For this healthcare provider, a developer's habit became a catastrophic risk.

The XM Cyber Difference (The "Gap" Fix):
The attacker entered the network via a compromised IoT device and identified machines broadcasting DHCPv6. By acting as a rogue DHCP server, the attacker positioned themselves as a "Man-in-the-Middle," intercepting traffic from a developer's laptop. They then exploited a known vulnerability to gain local shell access, and found unprotected private SSH keys sitting in the `C:\Users\Dev\Downloads` folder—legacy keys created for "temporary" cloud access that were never deleted.

The Blast Radius:
These keys provide immediate, password-less access to 200 Linux servers across the on-prem data center and the production cloud environment.

The XM Cyber Difference:
While traditional scanners looked for unpatched servers, they missed the **logical link** between a low-level user and the Domain Admin. XM Cyber identified this choke point and implemented a remediation plan that

The Hospital Where Every Employee was an (Accidental) Admin

Being in compliance means your policies are in place, but they don't always mean you are secure. This major medical center revealed that "anyone" could become a Domain Admin.

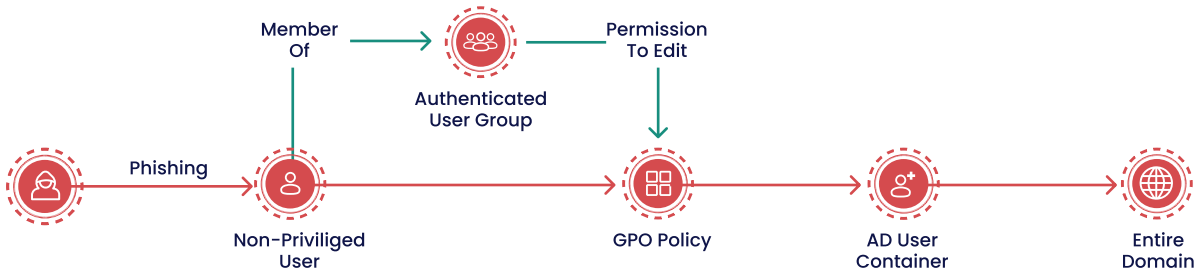
The Attack Path Breakdown:
A massive misconfiguration granted all users `ForceChangePassword` rights across the domain. An attacker compromised a non-privileged user, and reset the password of a Tier-1 IT helpdesk user and a Domain Admin account.

The Impact = Full Domain Dominance:
Within minutes, the attacker transitioned from a low-level phish to full administrative control over patient records and hospital systems.

The XM Cyber Difference:
While traditional scanners looked for unpatched servers, they missed the **logical link** between a low-level user and the Domain Admin. XM Cyber identified this choke point and implemented a remediation plan that prioritized hardening AD inheritance.

The GPO "Time Bomb"

Being in compliance means your policies are in place, but they don't always mean you are secure. This major medical center revealed that "anyone" could become a Domain Admin.



The Attack Path Breakdown:
An attacker found that the "Authenticated Users" group had write-access to the gPCFileSysPath attribute of a critical Group Policy Object (GPO). They changed the path to point to a malicious script and just waited for an Admin to log in.

The Blast Radius:
When a Domain Admin logs in, the malicious policy executes in their high-privilege context, granting the attacker a permanent backdoor with Admin rights.

The XM Cyber Difference:
The "logical hole" in most security strategies is assuming GPOs are immutable. XM Cyber flagged this hidden permission as a critical exposure, allowing the team to revoke the "Modify" rights before an attacker could weaponize the policy refresh cycle.