HUME IT

Client Success Story – Healthcare Industry

Discovering Cross-Platform Vulnerabilities in a Healthcare Technology Provider's Identity and Virtualization Stack

Client Profile

A nationally recognized healthcare technology provider specializing in electronic medical records (EMR), this organization operates a sophisticated internal IT infrastructure supporting over 13,000 users. Headquartered in the Midwest, the company plays a pivotal role in powering digital healthcare platforms across the U.S. The internal IT and Information Security teams, including cybersecurity leadership and virtualization SMEs, initiated a security assessment of their Active Directory that was later expanded to include the VMware vSphere environment after indicators of compromise suggested cross-platform vulnerabilities. While the organization maintained a generally mature security posture, the assessment revealed key blind spots, particularly in legacy authentication settings and virtualization layer protections, prompting corrective action in alignment with HIPAA compliance objectives.

The Challenge

The engagement began as a focused identity security posture review but quickly evolved when signs of deeper architectural risk surfaced. A potential attack path extending from Active Directory into the virtualization layer raised concern about cross-platform exposure. The organization needed visibility into both layers and a path to close the security gaps threatening the integrity of its electronic medical records infrastructure.

Top 3 Highest-Risk Discoveries

- **VMware Tools Vulnerability on Virtualized Domain Controllers**
  Allowed non-privileged AD users to exploit a known weakness and gain elevated access.
- **Lack of Network Segmentation Between AD and vSphere Components**
  Created an opportunity for lateral movement across trust boundaries.

- **Insecure Configuration of Virtualized Domain Controllers**
  Enabled potential guest-to-host privilege escalation from within critical systems.

Security Risks Identified

Initial findings in the identity platform revealed a potential lateral attack vector into the virtualization environment. Key risks included:

- **Outdated VMware Tools Installed on Domain Controllers**: Allowed exploitation of known privilege escalation vulnerabilities.
- **No Segmentation Between vSphere and AD Management Traffic**: Permitted unrestricted bidirectional access.
- **Lack of Hardening on Virtualized Domain Controllers**: Included insecure VM configuration parameters and excessive guest privileges.
- **Overlapping Administrative Access Rights**: Exposed both platforms to compromise from a single point of failure.

The Approach & Solution

The assessment scope was expanded in coordination with IT and InfoSec leadership to fully evaluate both AD and vSphere platforms. The following steps were taken:

- **Vulnerability Remediation**: Patched VMware Tools on all virtualized systems to close known exploit paths.
- **Network Segmentation Enforcement**: Introduced strict controls separating Active Directory components from vSphere management interfaces.
- **VM Hardening Standards Applied**: Hardened Domain Controllers by disabling unnecessary virtual features and restricting privileges.
- **Privileged Access Review Conducted**: Aligned roles and rights across platforms to reduce cross-platform administrative exposure.

The Impact

The organization successfully closed critical gaps that could have enabled lateral movement from Active Directory into the virtualization layer. Tangible outcomes included:

- Closed a high-risk privilege escalation vector affecting virtualized Domain Controllers
- Reduced likelihood of lateral compromise between identity and infrastructure layers
- Established enforceable segmentation policies separating identity and virtualization planes

- Improved HIPAA audit alignment by ensuring safeguards around systems housing electronic medical records

This cross-platform security posture improvement reinforced the organization’s commitment to safeguarding healthcare infrastructure while supporting ongoing compliance initiatives.

Strategic Takeaway

Platform-specific assessments are not always sufficient when risks extend beyond their boundaries. This engagement demonstrated the importance of interconnected reviews that uncover how weaknesses in one layer (identity) can cascade into another (virtualization). Securing modern enterprise environments requires a holistic view of privilege, configuration, and exposure across all critical systems.