BLOODHOUND ENTERPRISE

CASE STUDY

Regional Hospital System Fills Gap in Identity Risk Reduction

A U.S. Healthcare Organization Eliminated Hidden Privilege Escalation Chains with BloodHound Enterprise

Challenge

A Midwestern hospital system with more than 10 hospitals, along with a range of medical care centers, had a fragmented process of manual audits, penetration tests, and alerts from various security tools to discover vulnerabilities and attack paths.

They knew there was a bigger problem to solve, but they couldn't see it with their existing tech stack, let alone prioritize the most critical issues. And with their robust security culture—elimination of criticals, continuous scanning, and frequent communication outside the security silo—they knew it was time to find a tool that would move the needle.

Solution

They found that SpecterOps's BloodHound Enterprise, backed by its reputation from red teamers who use the open-source edition, was the key to unlocking total visibility across their Active Directory environment.

"When we saw the enterprise version, it immediately resonated as the right fit," the director of information security said.

With clear visibility, prioritization of attack paths, and proven remediation guidance, the security team was able to move quickly through hundreds of critical and high severity attack paths, **eliminating the 750+ attack paths across all their domains and counting.**

One type of attack path of particular concern involved Tier 0 administrators logging into lower tier systems and applications, which introduced risk to Tier 0 with the potential for credential compromise. They worked quickly to undo the privilege zone violations and reduce their exposure.

Once You Have Visibility, Prioritization Matters

The team's goals, identify hidden attack paths and reduce lateral movement opportunities, could only be achieved if they were able to prioritize the attack paths with the most potential for access to critical resources (aka disaster!).

Much like other traditional tools, such as vulnerability management, security teams can receive thousands of alerts which can quickly lead to burnout. Further, Identity teams outside of security are discouraged to make changes without knowing if the remediation worked, which makes sense considering a change to Active Directory could slow or even halt business processes.

After BloodHound Enterprise was deployed, the security team began work with their Active Directory team to implement fixes. The in-platform remediation guidance made for a smooth remediation process between the two teams. The guidance given per finding considers practicality; that is advice that won't break your Active Directory environment.

> **"The remediation guidance was practical, prioritized, and mapped directly to our environment. Rather than just telling us something was risky, BloodHound Enterprise gave us the exact steps needed to fix it."**
>
> **Director of Information Security**
> Regional Hospital System

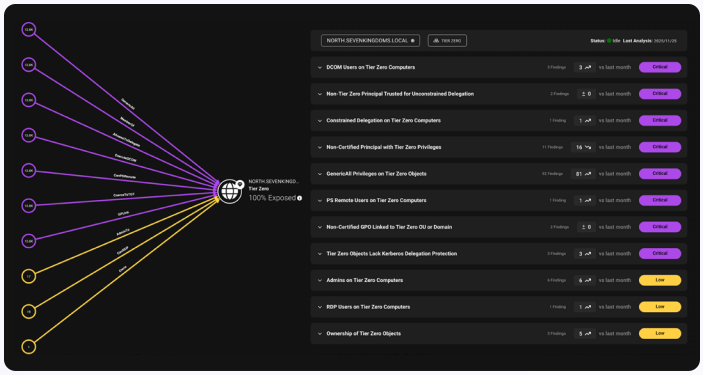
Protecting Sensitive Data in a Highly Regulated Industry

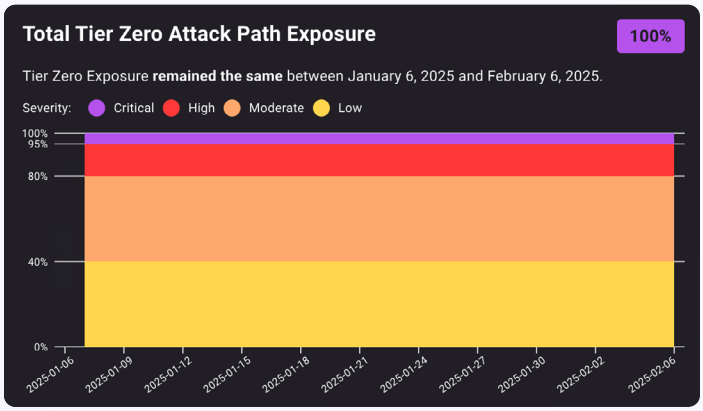
In healthcare organizations, security teams have the added pressure of complying with important patient protections, such as HIPAA. And for the regional hospital system, they also have to contend with new hospital acquisitions and varying needs of subsidiary organizations.

“Protecting patient data and ensuring continuity of care are at the heart of our mission,” the director said.

BloodHound Enterprise helps the security team safeguard the identity layer, which reduces the chance of ransomware or other attacks that could disrupt hospital operations. They now consider BloodHound an essential component to meeting security governance requirements.

“BloodHound gave us visibility into identity risks in newly integrated domains. Instead of waiting for long audit cycles, we could more quickly assess exposure and start remediation.”





Advice for Security Teams to Protect Identities and Reduce Security Risk

The Midwestern hospital system has something a lot of security teams need—a CISO that goes to bat for security readiness. With a strong security culture and a united IT department, the hospital system’s security team was able to execute the concept of Attack Path Management to its fullest extent.

Proactive security posturing by mapping the attack paths and remediating vulnerabilities before they’re exploited is an iterative endeavor. Culture, collaboration, and the right tools will set any security team up for success.

> **“Start by treating Attack Path Management as a core part of vulnerability management. Identity is a primary attack surface, and without attack path visibility, you’re flying blind. Also, prioritize collaboration with IT teams early—remediation often requires cross-functional partnership.”**
>
> **– Director of Information Security, Regional Hospital System**

Learn more at specterops.io/bloodhound-enterprise ›

BloodHound Enterprise Provides

- **Continuous attack path mapping**
- **Attack path choke point prioritisation**
- **Real-world remediation guidance**
- **Continuous security posture measurement**