BLOODHOUND ENTERPRISE

CASE STUDY

Large Hospitality Organization Welcomes AD Visibility

Challenge

Recently a large hospitality organization chose BloodHound Enterprise to address their lack of AD visiblity and to protect their organization from adversary privilege escalation and lateral movement. With globally distributed networks and operations in all corners of the world, this organization knew they had some challenging scenarios to address.

With 30+ far-flung sites operating over satellite communications, the customer made a strategic decision that each of these sites would have their own nearly identical Active Directory domain. This way they were able to achieve reduced security risk through separation and if any problems did arise, their AD operations team would be familiar with any given site's AD structure and able to resolve issues quickly.

In practice however, networks change rapidly causing the AD structures at each site to diverge from the standard. Further, the satcom-based communications for these sites meant that any AD visibility tool would have to be able to handle less than optimal connectivity scenarios.

The head of Offensive Security shared, "We knew we had to maintain the unique AD domains for separation, but we also had to support our business. Our biggest problem is that Microsoft AD does not provide the visibility we need to understand the AD configuration changes that occur for any given remote site. We needed to find a tool that would give us continuous visibility despite highly latent and limited bandwidth satcom connections."

Solution

This organization was familiar with BloodHound CE, utilizing it in their offensive security practice. As the Offensive Security lead said, "We had exposure to BloodHound Open-Source [Community Edition] and knew the AD visibility it could provide, but we needed an enterprise solution that could provide continuous scans. **BloodHound Enterprise provides the automated collection of each domain's privileges and relationships, both historical and current, and graphs the relationships to provide us the visibility we need."**

Upon trialing BloodHound Enterprise, the customer found BloodHound Enterprise's collector, SharpHound Enterprise, worked perfectly despite the limited satcom connectivity. But they knew the solution was for them when they immediately attained visibility across their entire AD forest.

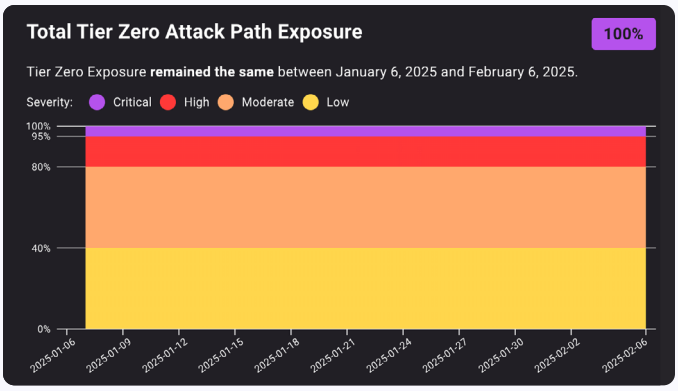
> **"We saw it right away. All the right information in one place. We were impressed that we could graphically expand any given AD group in any domain and see where they can go and what they have access to.**
>
> **In addition, we now can empirically measure our attack path exposure and as we address misconfigurations see our security posture improve."**

Offensive Security Lead
Large Hospitality Vendor

Attack Path Management for All

From the creators of BloodHound, an Attack Path Management solution that continuously maps and quantifies Active Directory and Azure attack paths.

Remove millions of attack paths within your existing architecture and eliminate the attacker's easiest, most dependable, and most attractive target.



Business Value

Use Case	Technical Capabilities	Customer Benefit
Detailed Visiblity Across 30+ Ad Domains	BloodHound Enterprise scales to provide visiblity across an unlimited number of AD domains/users and delivers clarity on AD's structure.	For the first time, enterprises can see and understand complex AD relationships, facilitating better architectural design and security team productivity gains.
High Latency, Low Bandwidth Connectivity	BloodHound Enterprise's SharpHound collector initially identifies every relationship within AD then scans continuously to relay any changes back to the BloodHound Enterprise platform.	BloodHound Enterprise's lightweight collector means organizations can achieve and maintain visiblity under any network scenario.
Empirical Attack Path Exposure	BloodHound Enterprise creates a baseline of AD, identifying each attack path and the number of users/computers that can traverse the path. Then as AD changes are made, BloodHound Enterprise continuously measures and reassess overall risk.	Enterprises understand their current state security posture of their AD environment and as they make improvements can see their posture improve.

> **"With 30+ AD domains each having connectivity limitations we did not hold out much hope for AD visibility, but BloodHound Enterprise surprised us exceeding our expectations. It is both a security solution and an AD visibility/design solution in one."**
>
> **– Offensive Security Lead, Large Hospitality Vendor**

Learn more at specterops.io/bloodhound-enterprise ›

BloodHound Enterprise Provides

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