TEXAS
The University of Texas at Austin

Everything's Bigger In Texas

Protecting the University of Texas – Austin's Active Directory is no small feat

CHALLENGE

The University of Texas – Austin's Active Directory environment serves 300K devices and 82K people daily. With a mature, experienced security staff, UT-Austin's CISO, Cam Beasley, knows the importance of securing the systems that grant access to students, researchers, and professors. Beasley's team performs regular penetration tests (both internal and third-party-led) on the UT-Austin environments to identify risks. However, in Beasley's words, he needed to "shed a light on their environment in a different way." It wasn't enough to see what an adversary could do at a point in time, he needed to see the full picture on a continuous basis.

SOLUTION

Having used BloodHound Free and Open-Source Software (FOSS), as an offensive tool to both conduct penetration tests and to teach students as part of the university's cyber-security programs, UT-Austin was very familiar with its ability to identify an AD Attack Path that can enable a red teamer to reach Tier 0 assets. When they learned that BloodHound Enterprise was available as a defensive tool that wasn't limited to Attack Paths from a single target principal to an objective, but instead it could continuously identify all AD Attack Paths from any target principal to any Tier 0 objective they had to take a look.

During their initial trial, BloodHound Enterprise immediately identified key Group Policy Objects, GPOs, that had been abandoned and forgotten, confirming Beasley's belief they needed to see the full picture.

Once purchased, an unanticipated benefit has been the collaboration BloodHound Enterprise has enabled between Beasley's security team and the AD Admins for UT-Austin. Beasley states "BloodHound illustrates the security findings with robust remediation steps utilizing AD vernacular, making it easier for our AD and security teams to work together and collaborate."

"We have been delighted with the simple, straightforward roll-out and rapid risk reduction BloodHound Enterprise has provided. We are sharing our experience with peers at other academic institutions," said Beasley. "It's a valuable new product and I like that they are responsive to feature requests. They are working with us to extend their role management capabilities to meet the different needs of an academic institution. Similarly, their new Splunk integration enables us to bring their findings into our core systems, allowing us to automate and reduce our response times."

CUSTOMER BENEFITS

UNPRECEDENTED VISIBILITY INTO ACTIVE DIRECTORY
Visualize privileges for instant clarity on AD architecture

BEST PRACTICES MADE PRACTICAL
Achieving and sustaining Tiered Administration, Least Privilege, and Credential Hygiene are now possible

ACTIVE DIRECTORY SECURITY FOR EVERYONE
Harden Active Directory against abuse and improve directory services availability

ELIMINATION OF 'BAND-AID' FIXES
Directly address the risk of Attack Paths at precise Choke Points rather than fighting misconfiguration debt

MEASURABLY IMPROVED SECURITY POSTURE
Meaningful, transparent measurements that illustrate the risk reduction gained from Attack Path Management

BLOODHOUND
ENTERPRISE

BLOODHOUNDENTERPRISE.IO

BLOODHOUND
ENTERPRISE

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
Enterprise-grade solution with minimal maintenance.	Delivered as a full SaaS solution with REST APIs, User Management, built-in training, reporting, signed binaries for local data collection, and enterprise support model with assigned customer success technical account manager.	Minimal setup and zero ongoing maintenance.
Continuous visibility of all AD Attack Paths.	Fully automated real-time data collection and analysis with Attack Path identification, prioritization based on Tier 0 exposure percentage, and risk trend reporting over time.	Always aware of AD exposure with real-time updates to environmental changes.
Empirical Attack Path Exposure for the security team and C-Suite.	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 reassesses overall risk.	Enterprises understand the current state security posture of their AD environment and as they make improvements can see their posture improve.

> "BloodHound illustrates the security findings with robust remediation steps utilizing AD vernacular, making it easier for our AD and security teams to work together and collaborate."
>
> *– CISO, University of Texas-Austin*

BLOODHOUND ENTERPRISE PROVIDES:

- Continuous Attack Path Mapping
- Attack Path Choke Point Prioritization
- Real-World Remediation Guidance
- Continuous Security Posture Measurement

BLOODHOUNDENTERPRISE.IO