BLOODHOUND ENTERPRISE

Fighting Fire with Fire

Eliminating AD Critical Paths to Tier 0 Assets

Global Top 5 Car Company's Loan Financing Firm Moves to Realtime Visibility of Cyber Exposure Risk with BloodHound Enterprise

CHALLENGE

It happens virtually without fail to enterprises around the globe. You hire a third-party security firm to run pen tests on your infrastructure with the intent of improving your SOC's response capabilities. The positive is that your Blue Team gets faster at responding... But the nasty side effect is you now spend countless hours eliminating the path the third party took to access domain admin privileges only to learn the next time you hire the third-party adversary simulation team they find more paths. It seems never-ending.

The CISO of the financing arm of a global top 5 car company grew tired of the challenge stating, "It ticked me off. We would fix the path the pen tester took to gain domain admin and then 20 minutes later they would find another path. I needed to fight fire with fire. I needed to see what the adversaries see and eliminate the critical paths to my Tier 0 assets."

SOLUTION

The CISO's third-party and internal pen testing teams were all using BloodHound open source to find paths to take control of their Active Directory, so naturally, he turned to BloodHound Enterprise. "I liked the visibility BloodHound open source provides, but it is designed for pen testers to find individual paths. I needed BloodHound Enterprise to continuously identify all Attack Paths, provide remediation best practices for my team, and enable the elimination of critical attack paths to reduce risk."

The CISO had three aha moments during their assessment of BloodHound Enterprise before they purchased. First, BloodHound Enterprise is a SaaS offering with minimal setup and zero maintenance for his team. Second, Bloodhound Enterprise provides visibility to all potential AD Attack Paths so that next year's external pen test would be both much more difficult for the testers and if they were able to penetrate, the security team would already have a documented remediation plan in process. The last aha moment, BloodHound Enterprise allows him to continuously publish their company's AD exposure to the C-Suite so that everyone knows the real-time impact of any changes to the company's environment. The CISO stated, "Our cyber posture will be visible on every executive's phone, so they are always aware and be part of the solution."

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

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 Enterprise lets us reduce risk by turning off the risk quickly. We needed a way to get ahead of these things and now we have it."

– CISO, Top 5 Car Maker's Loan Financing Firm

BLOODHOUND ENTERPRISE PROVIDES:

Continuous Attack Path Mapping

Attack Path Choke Point Prioritization

Real-World Remediation Guidance

Continuous Security Posture Measurement