# **BloodHound Enterprise**

## Reduce Risk in Your Identity and Directory Environments

Identity and directory environments have become the preferred entry points for adversaries. Once a user with privileged access has been compromised, an attacker can easily orchestrate a cyberattack by taking control of an organization's critical assets. Identity Attack Paths are trivial for threat actors to exploit, yet difficult for defenders to detect, and the root cause of significant risk within Active Directory (AD), Active Directory Certificate Services (ADCS) and Entra ID (formerly Azure AD) environments.

Adversaries use Identity Attack Paths to move laterally and escalate privilege, evading detection with ease as they attempt escalation to domain-level controls (known as Tier Zero). When AD, Entra ID and Azure are the backbone to nearly everything in your stack, guided visibility of your Identity Attack Paths and knowing the gaps of your directory hygiene is essential.

Due to the complexity of AD environments, years of accumulated technical debt and constant org changes, most companies lack the insights needed to identify and remediate their Identity Attack Path vulnerabilities. This opens the door for threat actors to easily compromise an organization's crown jewels.

95% of Fortune 1000 organizations have Attack Paths reachable via AD and Entra ID On average, over 70% of users in an AD domain have at least one attack path to Tier Zero and control over the enterprise

97% of breaches leverage an Identity Attack Path

.00DH0UND

Powered by SPECTEROPS

ENTERPRIS

SpecterOps pioneered the concept of Attack Path Management (APM) by creating and maintaining BloodHound since 2017.

Now, with BloodHound Enterprise, an adversarial view of how to exploit (and proactively manage) Identity risk in your AD, Entra ID, and hybrid environments can be visualized in a fully managed SaaS tool with remediation guidance, and improvements which are tracked over time.

BloodHound Enterprise continuously maps and quantifies Attack Paths within your existing architecture, exposes misconfigurations and reduces the allure of targeting directories as the preferred attack vector.

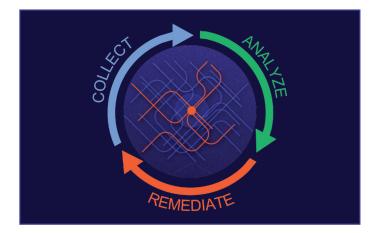
		TITANCORPLOCAL  Status: Idle Last Analysis: 2025-02-10 08:26 PST (GMT-0800)					
~		✓ Kerberoastable User Accounts	9 Findings ± 0 Critical				
		<ul> <li>Kerberos Delegation on Tier Zero Objects</li> </ul>	137 Findings 4 🐄 Critical				
Ť		✓ AS-REP Roastable User Accounts	S Findings ± 0 Critical				
ے ب	Accessor Hasschulstory Tier Zero	✓ Generic Write Privileges on Tier Zero Objects	357 Findings 8 🗚 Critical				
2	Contraction → MCCSECC → MCCSECCC → MCCSECCCC → MCCSECCCC → MCCSECCCC → MCCSECCCC → MCCSECCCC → MCCSECCCC → MCCSECCCCCC → MCCSECCCCCCCCC → MCCSECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC	✓ RDP Users on Tier Zero Computers	36 Findings ± 0 Critical				
0		✓ Write DACL Privileges on Tier Zero Objects	19 Findings ± 0 Critical				
а Ф	(m) / /// (m) / ///	<ul> <li>DCOM Users on Tier Zero Computers</li> </ul>	8 Findings 4 🔊 Critical				
ۥ	S/	<ul> <li>Write Owner Privileges on Tier Zero Objects</li> </ul>	18 Findings ± 0 Critical				
Reset View	(17)						

Visualize the complex connections and relationships in AD and Azure to understand where misconfigurations have exposed your organization's most valuable assets.

## **Key Benefits**

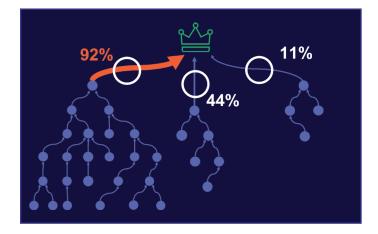
- Gain visibility into your Identity risk and exposure across your AD, ADCS, Entra ID, and hybrid environments.
- Eliminate years of technical debt from multiple generations of AD Admins, on-prem AD / hybrid complexities, and mergers & acquisitions.
- Continuously audit for new Identitybased risks introduced into your environment.
- Get insights on Attack Path risk and remediation progress over time.

### Why BloodHound Enterprise



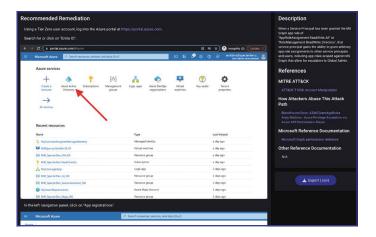
#### **Continuous Attack Path Mapping**

Identify your most critical Tier Zero or Control Plane assets, and then continuously identify every available Attack Path to understand how adversaries can move laterally and escalate privileges to compromise your environment. BloodHound Enterprise covers AD, Entra ID, and hybrid environments.



#### **Prioritized Attack Path Choke Points**

Analyze the millions of Attack Paths within your environment, identify the choke points that enable rapid risk reduction, and prioritize them based on the risk presented to your organization. This allows you to eliminate the largest amount of Attack Path risk with a single remediation.



#### Practical, Step-by-Step Remediations

Remove misconfiguration debt using guided remediations that walks your administrators through resolution processes screen-by-screen, eliminating the guesswork and ensuring practical and safe remediation.

To learn more, contact your SpecterOps representative or sign up for a demo to see how BloodHound Enterprise can help protect your organization's most critical assets: SPECTEROPS.IO

Understanding Posture Bioditional Enterprise analyzed to determine risk across your environment. Lateral movement and privilege escalation opportunities are analyzed to determine risk based on exposure (principals that can attack an object) or impact (what principals an object can attack). Learn more here.					Attack Path Summary Spectrolys identified that 20% of all principals in the TTANCOBPLOCAL environment have at least one vi attack path leading to the compromise of a Tier Zero principal and thus absolute control of the entire environment.					
Attack Paths		9, Search 🛛 🔗		Attack Paths		Findings		Tier Zero Objects		
Severity	Name 0	Category	Findings	Change 🛛 0	ЗM		982		219	
•	Large Default Groups with RDP Access				▲ 3M vs last 30 days					
۲	Kerberos Delegation on Tier Zero Objects	Kerberos			Total Tier Zero Attack Path Exposure 20%					
۲	AS REP Roastable User Accounts	Kerberos			Tier Zero Exposure decreased by 80% between January 1, 2025 and January 31, 2025. Severty: Critical High & Molennie & Low 120: 1					
۲	Kerberoastable User Accounts	Kerberos								
۲	DCOM Users on Tier Zero Computers	Tier Zero			814 -	294				
۲	Logons from Tier Zero Users	Tier Zero					_			
۰	Write DACL Privileges on Tier Zero Objects	Tier Zero								
۲	Non Tier Zero Principals with DCSync Privileges				and and and a	in ser	and and and and	and see	·	
•	Legacy SID History on Tier Zero Objects									
۲	Ownership Privileges on Tier Zero Objects				Group Completeness	Ses	Session Completeness o			
•	RDP Users on Tier Zero Computers	Tier Zero			85%		85	%		
۲	Non Tier Zero Principal Trusted for Unconstrained Delegation	Tier Zero								
۲	Write Owner Privileges on Tier Zero Objects									
•	Non Tier Zero Principals with ADCS									

#### **Security Posture Measurement**

Establish a baseline of your security posture, reassess risk and track improvements across all your directory environments over time.

"The BloodHound Enterprise team approached the problem differently, focusing first on Attack Path exposure to Tier Zero. They used the same language as our assessment experts, prioritized issues on risk, and included detailed remediation advice in each finding."

– Ryan Gray, Security Engineering Manager, Woodside Energy