BloodHound Enterprise - FedRAMP[®] High Authorized Reduce Risk in Your Identity and Directory Environments

Identity is a prime target for adversaries. Once a privileged account is compromised, attackers can quickly seize control of an organization's critical assets. Identity Attack Paths are easy for threat actors to exploit but hard for defenders to detect, posing major risks in Active Directory (AD), Active Directory Certificate Services (ADCS), and Entra ID environments.

Attackers use these paths to move laterally, escalate privileges, and evade detection, aiming for privileged access (known as Tier Zero) control. Since AD, Entra ID, and Azure underpin most systems, understanding Attack Paths and directory hygiene is crucial to mitigating identity risk.

However, the complexity of organizations' hybrid identity footprint, years of technical debt, and constant organizational changes leave most companies blind to these vulnerabilities—making it easier for attackers to breach critical assets.

97% of breaches leverage an Identity Attack Path Over 70% of users in an AD domain have at least one attack path to Tier Zero and control over the enterprise Fixing a single priority choke point can remove 300,000 attack paths

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

BloodHound Enterprise (BHE) provides an adversarial perspective on Identity risk in AD, Entra ID, and hybrid environments. This fully managed SaaS solution visualizes Attack Paths, offers remediation guidance, and tracks improvements over time.

BHE continuously maps and quantifies Attack Paths, identifies misconfigurations, and reduces the impact of targeting identities as the preferred attack vector.

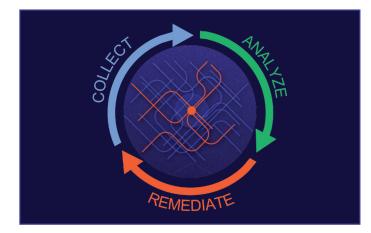
4.7K 4.7K		TITANCORP.LOCAL Status: Idle	Last Analysis: 2025-02-10 08:26 PST (GMT-0800)
		V Kerberoastable User Accounts	9 Findings ± 0 Critical
		 Kerberos Delegation on Tier Zero Objects 	137 Findings 4 🐄 Critical
	itancorplocal īer Zero 00% Exposed ●	✓ AS-REP Roastable User Accounts	5 Findings ± 0 Critical
4.7K HasSiDHiatory CoerceToTOT		✓ Generic Write Privileges on Tier Zero Objects	357 Findings 8 🕫 Critical
4.7K ASCREECT		 RDP Users on Tier Zero Computers 	36 Findings ± 0 Critical
		 Write DACL Privileges on Tier Zero Objects 	19 Findings ± 0 Critical
		 DCOM Users on Tier Zero Computers 	8 Findings 4 🕫 Critical
		✓ Write Owner Privileges on Tier Zero Objects	18 Findings ± 0 Critical

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

Key Benefits for Government Security & Identity Teams

- Gain visibility into your Identity risk and exposure across your entire AD, ADCS, Entra ID, and hybrid environment enabling security teams to enforce consistent policies and control.
- Helps agencies meet critical compliance requirements (such as, NIST CSF, NIST 800-171, and NIST 800-53) through continuous monitoring of Identity Attack Path exposure.
- Get insights on Attack Path risk and remediation progress over time
- Enable agencies that require FedRAMP High Authorization (achieved December 2024 via Palantir FedStart) to utilize BHE at scale to enhance their mission in protecting high-value assets

Why BloodHound Enterprise



Continuous Attack Path Mapping

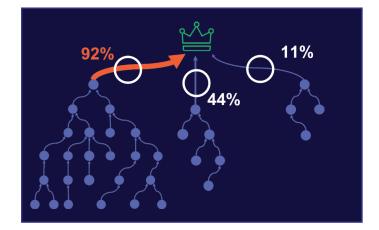
Identify your most critical Tier Zero or Control Plane assets, and then continuously identify every available Attack Path to understand how adversaries can move laterally and escalate privileges to compromise your environment.

Ising a Tier Zero user account, log into the Azur learch for or click on "Entra ID".	e portal at https://portal.azure.com.		When a Service Principal has been granted the Graph age role of "AppRoleAssignment.ReadWrite.All" or "RoleManagement.ReadWrite.Directory", that
O (a portal azure com/ilhome Microsoft Azure P Search resources services; a	ad docs (G+/)		Ro (2) Update i service principal agrines recording under service principal agrines the ability to grant arbiti app role assignments to other service principal expectenders. Graph that allow for exclusions of obbal Admin Graph that allow for exclusions of obbal Admin
Azure services		-	References
+ 🚸 📍	🖾 👗 📀	📮 😗 🍄	MITRE ATT&CK
Create a Azure Active Subscriptions resource Directory	Management Logic apps Azure DevOps groups organizations	Virtual Key vaults Terant machines properties	ATT&CK T1098: Account Manipulation
→ All services			How Attackers Abuse This Attack Path BloodHound Docs: AZMOGrienAppRoles Andy Robbins - Azure Privilege Escalation via Azure API Permissiona Abuse
At services Recent resources Name	Tore	Last Viewed	Path BloodHound Docs: AZMGGrantAppRoles Andy Robbins - Azure Privilege Escalation via
Recent resources	Type Managed Identity	Last Viewed a day ago	Path BloodHound Docs: AZM0GrienAppRoles Andy Robbins - Azure Privilege Escalation via Azure API Permissions Abuse
Recent resources			Path Biooditound Docs: AZMGGentAppRoles Arry Mohans - Arure Priviley Escalation via Arure API Permissions Abuse Microsoft Reference Documentatio
Recent resources Name & MyCostDamAssgmetManagetBenthy	Managed Identity	a day ago	Path Biodritound Does, AZMGTeerAppBoles Aray Robins, Azur Printing Exclusion vi Azur AD Versission Adue Microsoft Reference Documentatic Marsach Graph permissions reference
Recent resources Name V MyCostburksgree/Maragettenty BitSgreen/Centilin1-51	Managed Identity Virtual machine	a day ago a day ago a day ago a day ago	Path Biodification discres. ADM/GlassrApplicits Aray fieldsmin - Aray In Printing Floatedies via Aray APP Printing - Aray Printing - Aray Microsoft Reference Documentation Microsoft Reference Documentation
Recent resources Tore Store Res Res Res Res Res Res Res R	Managed Identity Witsal machine Resource group Subscription Logic app	a day ago a day ago a day ago a day ago 2 daya ago	Path Biodification discres. ADM/GlassrApplicits Aray fieldsmin - Aray In Printing Floatedies via Aray APP Printing - Aray Printing - Aray Microsoft Reference Documentation Microsoft Reference Documentation
Recent resources Term	Managed Identity Vitraal machine Resource group Subscription Logic app Resource group	a day ago a day ago a day ago a day ago 2 daya ago 2 daya ago 2 daya ago	Path Bender Genz Abstrammen Genz Abstrammen Genz Abstrammen Abstrammen Abstrammen Genz Microsoft Reference Documentation Other Reference Documentation Not
Recent resources New Subscriptions and the second	Managed Mentry Virtual machine Resource group Subscription Logic app Resource group Resource group	a day ago a day ago a day ago a day ago a day ago 2 days ago 2 days ago 2 days ago	Path Biodification discres. ADM/GlassrApplicits Aray fieldsmin - Aray In Printing Floatedies via Aray APP Printing - Aray Printing - Aray Microsoft Reference Documentation Microsoft Reference Documentation
Recent resources Term	Managed Identity Vitraal machine Resource group Subscription Logic app Resource group	a day ago a day ago a day ago a day ago 2 daya ago 2 daya ago 2 daya ago	Path Bender Genz Abstrammen Genz Abstrammen Genz Abstrammen Abstrammen Abstrammen Genz Microsoft Reference Documentation Other Reference Documentation Not

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



Prioritized Attack Path Choke Points

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



Security Posture Measurement

Establish a baseline of your identity 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