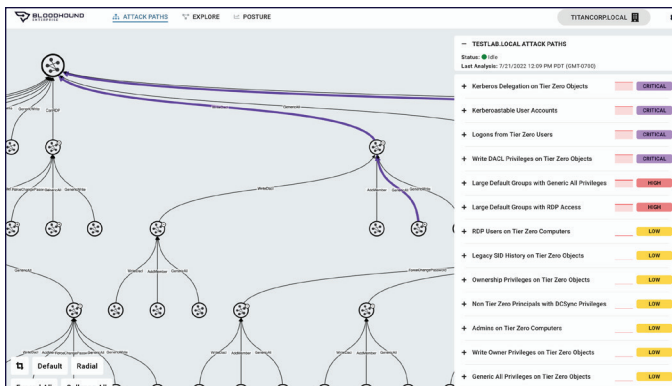


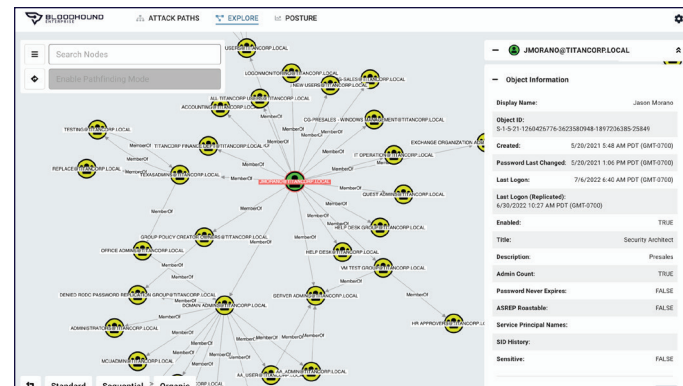
“Identity is the new perimeter,” but adversaries have been exploiting Identity for decades. Identity Attack Paths are trivial for attackers to abuse, and the root cause of significant Identity risk in Active Directory and Entra ID. Adversaries use these Attack Paths to move laterally and escalate privilege, evading detection with ease.

SpecterOps has pioneered the abuse, research and visualization of Attack Paths through BloodHound for the last decade. 95% of Fortune 1000 organizations have Attack Paths through Active Directory and Azure. Now is the time to think about this problem differently.

Introducing BloodHound Enterprise, the adversary view of how to exploit (and proactively manage) Identity risk in your Active Directory and Azure environments. You cannot fix what you cannot see, start by continuously mapping all Identity Attack Paths across your Enterprise.



Identify and quantify the Attack Path choke points that will eliminate the most risk to your critical assets.



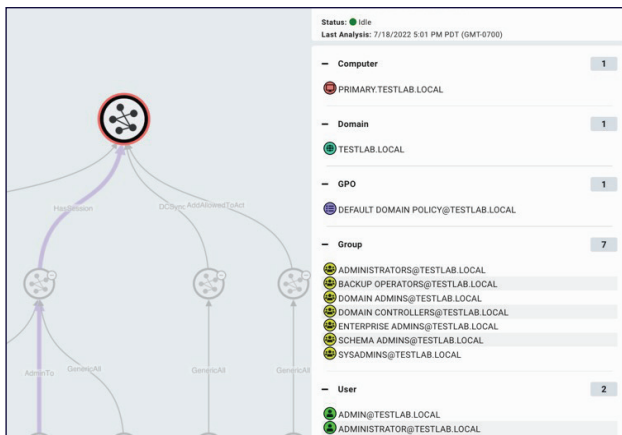
Visualize the complex connections and relationships in AD and Azure to understand where misconfigurations have exposed your organization's most valuable assets.

## Benefits:

- Measure your Identity risk and exposure in Active Directory and Entra ID
- Identify Choke Points to remediate millions of Attack Paths with individual fixes
- Eliminate years of technical debt
- Continuously audit for new Identity risk introduced into your environment

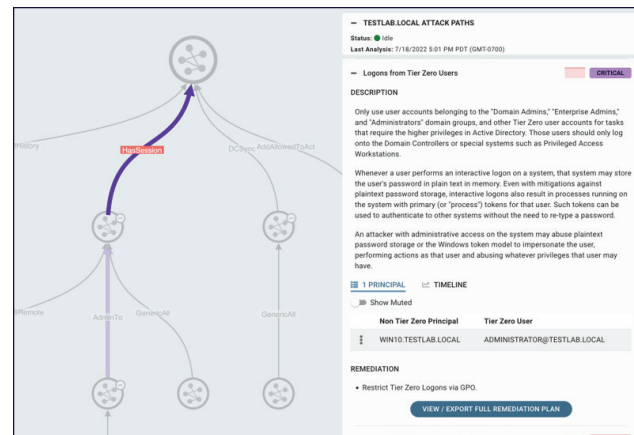
**“The BloodHound Enterprise team approached the problem differently, focusing first on Attack Path exposure to Tier Zero. They used the same language as our assessment experts, prioritized issues on risk, and included detailed remediation advice in each finding.”** – Ryan Gray, Security Engineering Manager,

Woodside Energy



## Continuous Attack Path Mapping

After automatically identifying critical Tier Zero or Control Plane assets, BloodHound Enterprise continuously identifies every available Attack Path to understand how adversaries can move laterally and escalate privilege to compromise your environment.



## Prioritized Attack Path Choke Points

BloodHound Enterprise analyzes the millions of Attack Paths in your environment, identifies the choke points that enable rapid risk reduction, and prioritizes them based on the risk presented to your organization. This allows you to eliminate the largest amount of Attack Path risk with a single fix.

### Add Secret to Tier Zero Service Principal or App

**Recommended Remediation**

Remediation of this finding will depend on whether the non Tier Zero principal has been granted a tenant-scoped, service principal-scoped, or app-scoped role assignment. Additionally, this finding may be produced when the non Tier Zero principal has been granted explicit ownership of the service principal or app.

**Removing Tenant-scoped role assignment:**

- Using a Tier Zero user account, log into the Azure portal at <https://portal.azure.com>.
- Search for or click on "Azure Active Directory".

The screenshot shows the 'Members' tab in the Azure portal. It displays a list of members with columns for 'Name', 'Role', and 'Permissions'. The 'Name' column shows various service principals and user accounts. The 'Role' column shows the assigned roles, and the 'Permissions' column shows the specific permissions granted to each member.

**Description**

Azure provides several systems and mechanisms for granting control of securable objects within Azure Active Directory, including tenant-scoped admin roles, object-scoped admin roles, explicit object ownership, and API permissions.

When a principal has been granted "Cloud App Admin" or "App Admin" against the tenant, that principal gains the ability to add new secrets to all Service Principals and App Registrations. Additionally, a principal that has been granted "Cloud App Admin" or "App Admin" against, or explicit ownership of a Service Principal or App Registration gains the ability to add secrets to that particular object.

**References**

**MITRE ATTACK**

- ATTACK T1098: Account Manipulation

**How Attackers Abuse This Attack Path**

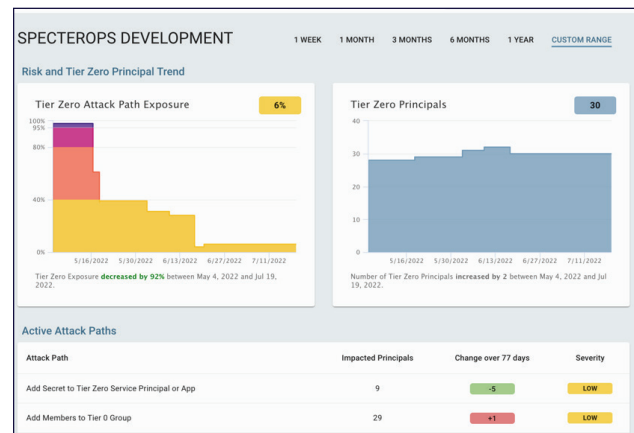
- Andy Robbins - Azure Privilege Escalation via Service Principal Abuse

**Microsoft Reference Documentation**

- Assign Azure AD roles at different scopes

## Practical, Step-by-Step Remediations

Remove misconfiguration debt rapidly using the guided remediations that walk administrators through resolution screen by screen.



## Security Posture Measurement

Establish a baseline and track progress as administrators change Azure and Active Directory, reassessing risk over time.

Breaches are inevitable, but impactful breaches are not.  
Sign up for a demo at  
**BLOODHOUNDENTERPRISE.IO**



[bloodhoundenterprise.io](https://bloodhoundenterprise.io)