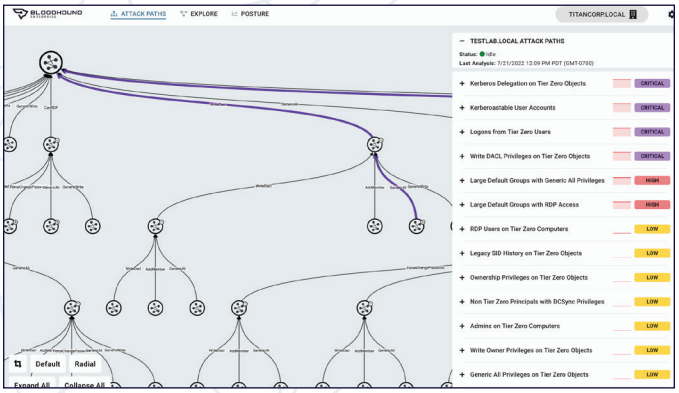
BLOODHOUND ENTERPRISE

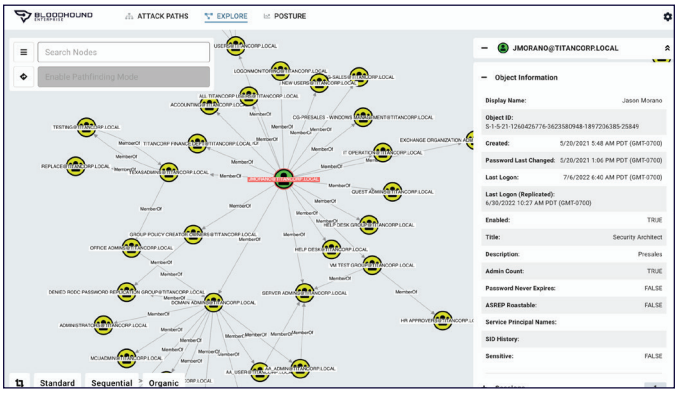
95% of enterprises rely on Active Directory & Azure Active Directory as a foundation for operations, making them ideal targets for the adversary. Chains of abusable privileges and configurations within these systems form thousands of Attack Paths that allow the adversary to move laterally and escalate privilege with ease. Where do you start?

Unfortunately, most products today think in lists — checking thousands of generic configuration issues, burying your team in work. Conversely, attackers think in graphs and can quickly and efficiently find a path to Control Plane or Tier Zero assets. This is where BloodHound Enterprise can help.

BloodHound Enterprise uses this same adversary perspective to continuously map and quantify identity Attack Paths in your hybrid environment. It isolates the most critical assets in your directory from attack by identifying prioritized Attack Path choke points and provides step-by-step guidance to rapidly remove thousands of Attack Paths.



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



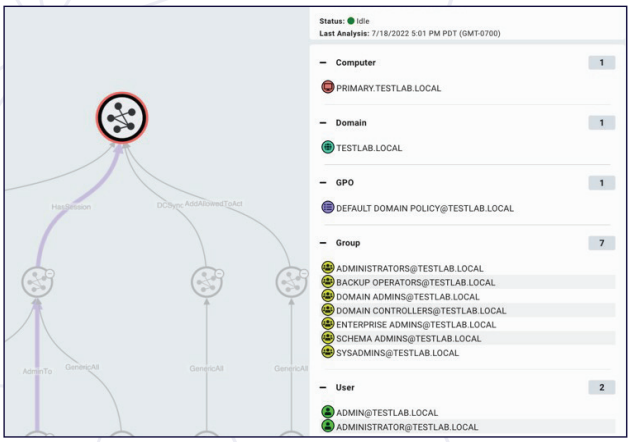
Visualize the complex connections and relationships in AD and Azure to understand where misconfigurations have exposed your organization's most valuable assets.

Benefits:

- Measure the risk of every Attack Path.
- Identify privilege chokepoints to remove the largest number of Attack Paths.
- Prioritize Attack Paths for remediation by collective risk reduction.
- Minimize remediation efforts and eliminate misconfiguration debt.

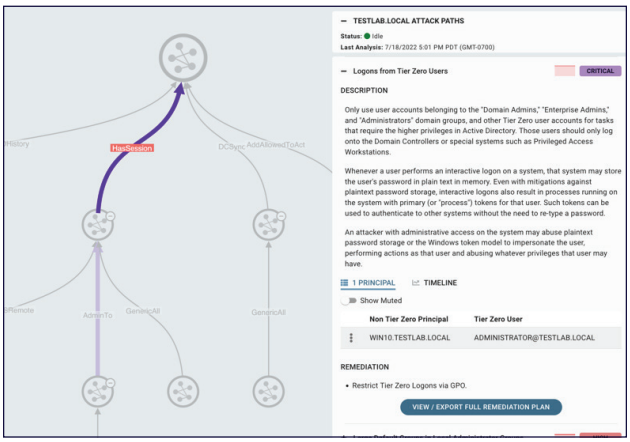
"The BloodHound Enterprise team approached the problem differently, focusing first on attack path exposure to Tier Zero. They used the same language as our assessment experts, prioritized issues on risk, and included detailed remediation advice in each finding."

– Ryan Gray, Security Engineering Manager, Woodside Energy



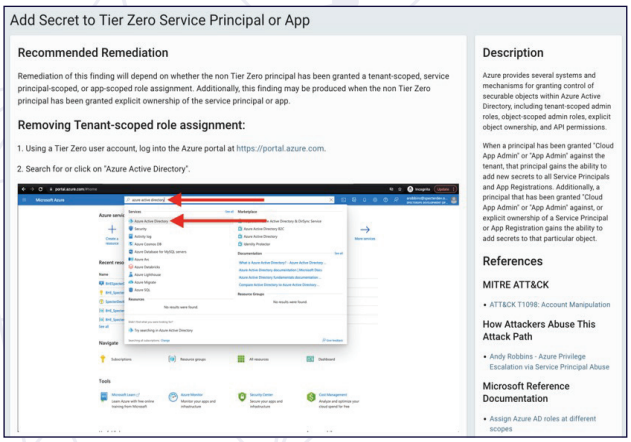
Continuous Attack Path Mapping

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.



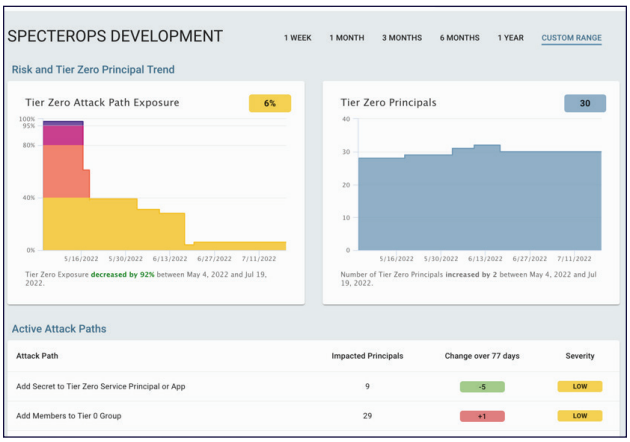
Prioritized Attack Path Choke Points

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.



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.

BloodHound Enterprise is agent-less, requires no privilege, and deploys in under 30 minutes. Sign up for a demo at **BLOODHOUNDENTERPRISE.IO**