Go Beyond Tier Zero with Multi-Tier Analysis in BloodHound

Reduce business risk by managing and analyzing critical assets and services outside of Tier Zero

Microsoft has long supported a model of tiering assets into secure management categories as part of their privileged access strategy. The most critical assets in Active Directory and Entra ID, that have direct or indirect administrative control over the environment, are classified as Tier Zero (or the Control Plane).

Securing Tier Zero is fundamental to identity security and a priority for practitioners and security leaders to protect and prevent consequential data breaches, escalation of an attacker within directory environments, or other malicious activity designed to take down an organization.

Beyond Tier Zero, other business critical assets likely require similar scrutiny and visibility. For example, health records at a regional hospital or a code repository at a tech company. **These assets deserve as much scrutiny as Tier Zero to reduce business risk, such as loss of reputation or loss of revenue, which is why we're introducing Multi-Tier Analysis.**

Tier Zero will continue to be a group of critical assets for attack path analysis, but teams will be able to add additional tiers as unique to each organization's priorities. Tier 1 assets may include things like HIPPA servers, databases with customer information, or PCI DSS payment systems that require 100% uptime.

With Multi-Tiering, teams can identify an asset, determine its appropriate tier, and apply the correct label. Additional multi-tiering functionality will be available later in the year that will allow the same attack path analysis to be conducted on those assets outside of Tier Zero.

The analysis will include a risk score, assess severity, classify the attack path, offer remediation guidance, and highlight any connections to Tier Zero.

Multi-Tiering enables customers to go further into the attack graph with:

- Segmenting assets based on their business priorities and environment.
- Protect any asset with BloodHound Enterprise's (BHE) rigorous analysis and visualization.
- New views to understand potential attack paths and quantify security risks by tier.
- A holistic view of all the assets that make up an organization's critical functions.

BLOODHOUND ENTERPRISE

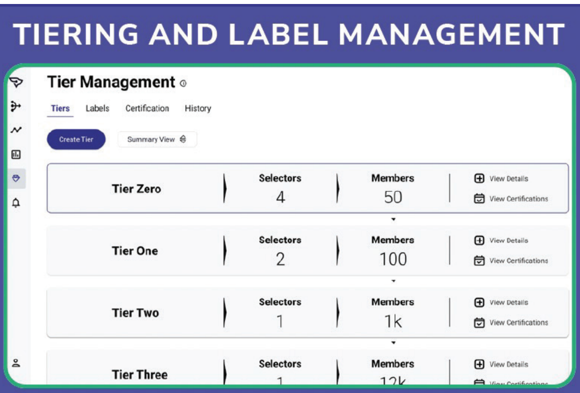
Powered by SPECTEROPS

Getting Started

Multi-Tiering includes two components: management and analysis. Available in June 2025, Multi-Tier Management will allow users to create a tier structure outside of Tier Zero BHE and apply labels to assets to group into Tier 1, Tier 2, etc. This functionality will be available to all users of BHE.

A follow-up, to come later this year, will be Multi-Tier Analysis. Once all the assets outside of Tier Zero that need to be protected have been identified, those assets can be analyzed for potential attack paths, just like Tier Zero assets. With a subscription to Multi-Tier Analysis, BloodHound Enterprise customers will be able to view assets and attack paths by tier to shore up adequate security measures.

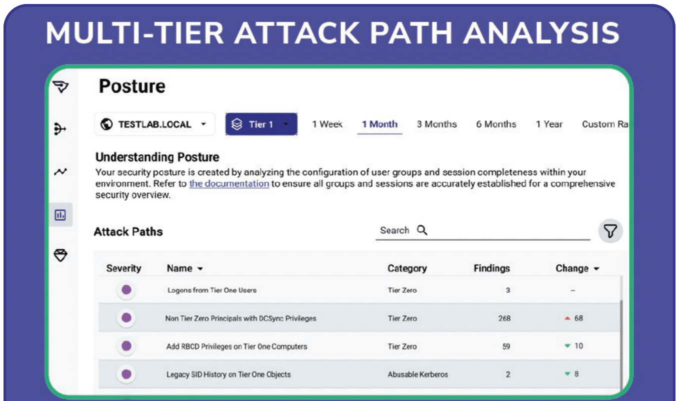
TIERING AND LABEL MANAGEMENT



	Selectors	Members
Tier Zero	4	50
Tier One	2	100
Tier Two	1	1k
Tier Three	1	12k

- Define Tiers based on your identity security architecture
- Create Labels to group identities and resources logically (e.g., “PCI assets,” “HIPAA enclave”)
- Track who, when, and how assets are assigned tiers with labels for complete visibility

MULTI-TIER ATTACK PATH ANALYSIS



Understanding Posture

Your security posture is created by analyzing the configuration of user groups and session completeness within your environment. Refer to the documentation to ensure all groups and sessions are accurately established for a comprehensive security overview.

Attack Paths

Severity	Name	Category	Findings	Change
●	Logons from Tier One Users	Tier Zero	3	--
●	Non Tier Zero Principals with DCSync Privileges	Tier Zero	268	▲ 68
●	Add RBCD Privileges on Tier One Computers	Tier Zero	59	▼ 10
●	Legacy SID History on Tier One Objects	Abusable Kerberos	2	▼ 8

- Analyze Attack Paths across Tiers and Labels
- Identify choke points where attackers can bypass security boundaries
- Ensure your tiered architecture works as designed—no gaps, no blind spots

Summary

The Multi-Tiering functionality in BloodHound enables your teams to manage and analyze any asset considered critical to your business, reducing the risk of access and escalation by attackers. To see how this tiering functionality can work for your organization, book a meeting with your SpecterOps representative or head to specterops.io/get-a-demo.

To learn more about Multi-Tier Analysis in BloodHound Enterprise, visit specterops.io/get-a-demo