



Mission: Compliance and Maturity

COMPLIANCE FRAMEWORKS

BloodHound Enterprise for Government enables compliance for frameworks that require users to maintain separate privileged accounts from their standard user accounts. Example compliance frameworks include:

NIST CSF v1.1

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes

- PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

NIST CSF 2.0

- PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties
- ID.RA-03: Internal and external threats to the organization are identified and recorded

NIST SP 800-53 Rev. 5

- AC-5: Separation of Duties
- AC-6: Least Privilege

MATURITY MODELS

BloodHound Enterprise for Government provides Optimal Visibility, Analytics, and Risk Assessment maturity to your organization for implementing Zero Trust for Identities.

CISA *Zero Trust Maturity Model, Version 2.0, April 2023*

- Section 5.1 Identity, Function - Risk Assessment, Maturity Level Optimal, "Agency determines identity risk in real time based on continuous analysis and dynamic rules to deliver ongoing protection."
- Section 5.1 Identity, Function - Visibility and Analytics Capability, Maturity Level Optimal, "Agency maintains comprehensive visibility and situational awareness across enterprise by performing automated analysis over user activity log types, including behavior-based analytics."

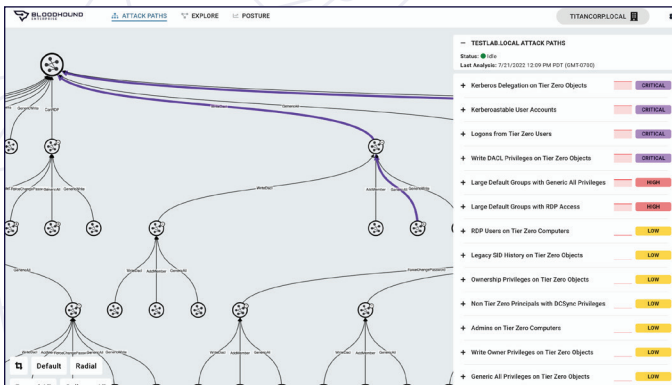
DoD *Zero Trust Strategy, October 2022*

- Target Level - User: 1.1 User Inventory (Satisfies)
- Target Level - User: 1.2 Conditional User Access (Enables/Validates)
- Target Level - User 1.4 Privileged Access Management (Enables/Validates)
- Target Level - User: 1.7 Least Privileged Access (Satisfies)

Identity Attack Paths are the easiest and most reliable technique adversaries use to gain complete control of your organization. Chains of abusable privileges and configurations within Azure and Active Directory managed by IAM solutions form thousands of Identity Attack Paths that enable lateral movement and privilege escalation.

With hybrid networks, cloud-based applications, and zero trust initiatives, the world is transforming to identity centric security. However, IAM frameworks and policies don't protect against the prevalent abuse of legitimate identities.

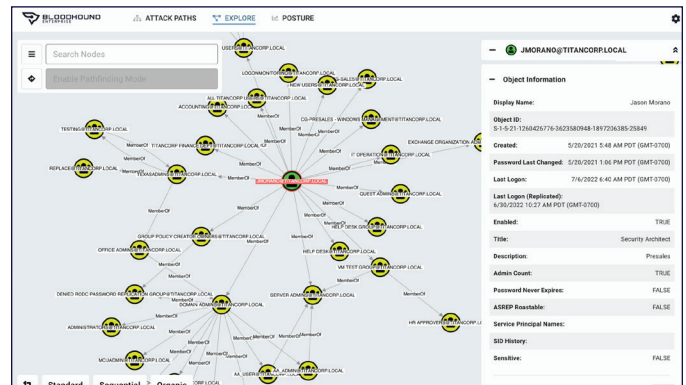
For enterprise security leaders who want the best solution to protect their organization, BloodHound Enterprise delivers the first-of-its-kind Identity Risk Management platform to identify and eliminate millions of Identity Attack Paths. By continuously identifying strategic Attack Path choke points and providing practical, precise, and safe remediation guidance, BloodHound Enterprise empowers security teams to remove identity privilege escalation risks efficiently and effectively.



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

Benefits:

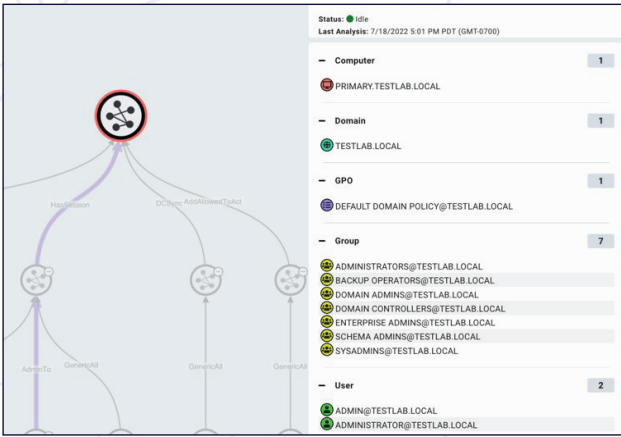
- Measure the risk of every Attack Path.
- Identify privilege chokepoints to remove the largest number of Attack Paths.
- Prioritize Attack Paths for remediation by collective risk reduction.
- Minimize remediation efforts and eliminate misconfiguration debt.



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

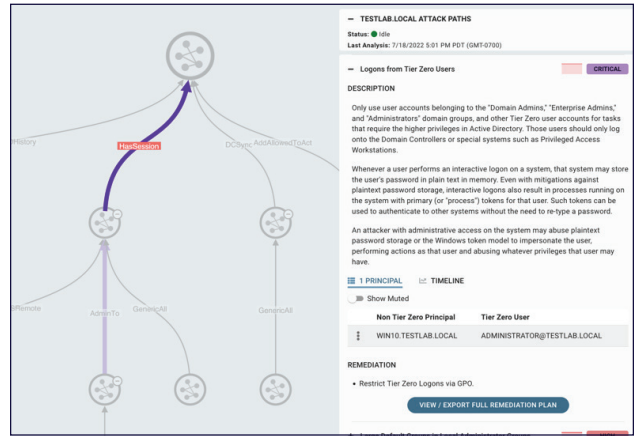
“The BloodHound Enterprise team approached the problem differently, focusing first on attack path exposure to Tier Zero. They used the same language as our assessment experts, prioritized issues on risk, and included detailed remediation advice in each finding.”

– 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'.

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.

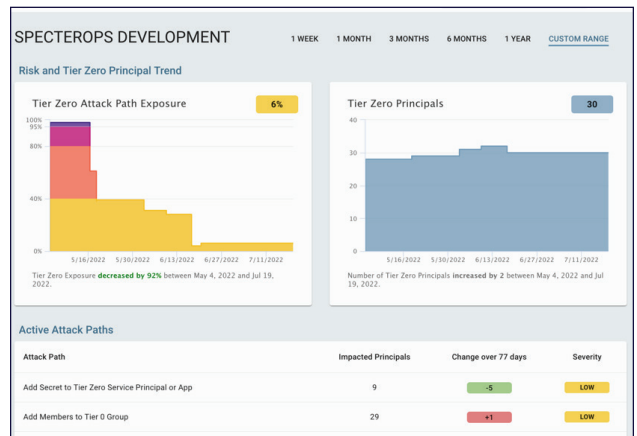
When a principal has been granted 'Cloud App Admin' or 'App Admin' against the tenant, that principal gains the ability to add new secrets to all Service Principals and App Registrations. Additionally, a principal that has been granted 'Cloud App Admin' or 'App Admin' against, or explicit ownership of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

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

