Photo courtesy of Woodside Energy

BLOODHOUND ENTERPRISE

Sustaining and Continuous Verification of Tier 0 with BloodHound Enterprise

CHALLENGE

As Australia's leading natural gas producer, Woodside places significant importance on the resiliency of its technology platforms and recognises Active Directory as a pervasive part of the IT landscape that ransomware operators have used to execute attacks at other organisations. After an initial Active Directory security assessment and completion of tactical improvements, Woodside commenced implementing Microsoft's Enterprise Access Model as a sustainable, comprehensive solution. On completing the first milestone (Tier 0), a critical question arose: In a complex operating environment, how can Woodside sustain Tier 0 by ensuring subsequent changes in Active Directory do not compromise its integrity by unintentionally opening attack paths from lower tiers?

Ryan Gray, Woodside Cyber Security Engineering Manager, shared, "We spent significant effort designing, building, and operationally adopting Tier 0 and needed to find a way to sustain it. Maintaining Tier 0 is challenging because, without full system awareness, it is possible to create unintentional privilege elevation paths. We needed an Active Directory security solution that understands the tiering model, that provides a high degree of certainty of the integrity of tiers and presents prioritised, actionable recommendations for paths that do exist. In surveying the market, we found that many solutions simultaneously overloaded us with insufficiently prioritised AD configuration problems from the entire AD environment. The solutions lacked technically sound advice on how to resolve each problem and, in many cases, failed to identify the issues our pen-testing engagements were finding. Such solutions leave us with a list of problems, and don't priortise on where to start."

SOLUTION

When BloodHound Enterprise launched in 2021, Woodside quickly realised this was something different. Gray revealed, "The BloodHound Enterprise team approached the problem differently, focusing first on attack path exposure to Tier 0. They used the same language as our assessment experts, prioritised issues on risk and included detailed remediation advice in each finding. We immediately recognised their level of expertise in this problem space."

While Woodside made their AD resilient, with enterprise environments changing daily, it is not enough to build the Enterprise Access Model - you must work hard to maintain it. With a simple deployment, BloodHound Enterprise rapidly mapped Woodside's environment and helped them identify critical Attack Paths that they may have otherwise missed. Gray commented, "Without Bloodhound Enterprise, we would have been relying solely on our periodic expert assessments. Now we're able to monitor the exposure of tiers daily and act on any issues BloodHound Enterprise detects rapidly."

With BloodHound Enterprise, Woodside can continuously identify newly created, unintentional Attack Paths and act rapidly to reduce risk.

Woodside Energy

BLOODHOUND ENTERPRISE

Attack Path Management for All

From the creators of BloodHound, an Attack Path Management solution that continuously maps and quantifies Active Directory and Azure Attack Paths. Remove millions of Attack Paths within your existing architecture and eliminate the attacker's easiest, most dependable, and most attractive target.

BUSINESS VALUE

USE CASE	TECHNICAL CAPABILITIES	CUSTOMER BENEFIT
Tier 0 Resiliency through Validation of AD Changes	BloodHound Enterprise continuously maps Attack Paths to Tier 0, providing near-immediate visibility to any unintentionally created Attack Paths from AD changes.	The ability to sustain Tier 0 resiliency, eliminating opportunities for adversaries to move laterally and gain control of AD.
Attack Path Choke Point Mapping	BloodHound Enterprise identifies key choke points, the specific privilege or misconfiguration that allows you to eliminate the largest number of Attack Paths.	Clear, precise prioritisation of where to mitigate risks, optimising efforts by focusing on the changes that will have the most significant impact.
Tier 1 and Critical System Resiliency	In addition to automatically identifying Tier 0 systems, BloodHound Enterprise allows administrators to specify both Tier 1 and critical system targets for continuous Attack Path mapping.	In addition to sustaining Tier 0 resiliency, enterprises can identify and eliminate Attack Path exposure to other key systems.
Attack Path Remediation	BloodHound Enterprise provides detailed, real-world remediation guidance.	Enterprises can act quickly and with confidence that the remediation steps will eliminate risks.

> 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. We immediately recognized their level of expertise in this problem space."

BLOODHOUND ENTERPRISE PROVIDES:

- Continuous Attack Path Mapping
- Attack Path Choke Point Prioritization
- Real-World Remediation Guidance
- Continuous Security Posture Measurement