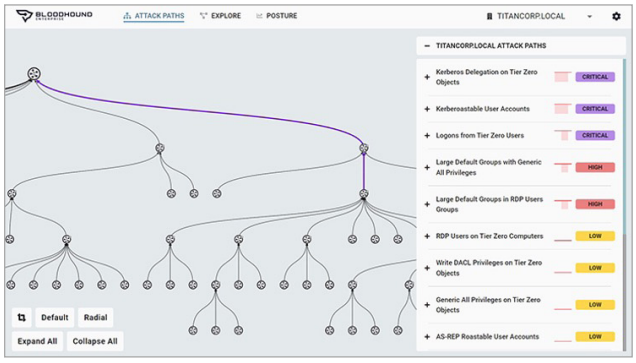
Sicherheitsbewertung von Active Directory

Mit SpecterOps BloodHound Enterprise Angriffspfade minimieren und Active Directory und Azure absichern

Eine kritische Komponente beim Schutz von Active Directory (AD) und Azure vor Cyberangriffen ist das Identifizieren und Absichern der Angriffspfade, die Angreifer zum Infiltrieren Ihrer AD Umgebung nutzen könnten. Das dürfte in Anbetracht der Tatsache, dass mehr als 95 Millionen AD-Benutzerkonten jeden Tag angegriffen werden, auch kaum verwunderlich sein. Aber woher wissen Sie, welche Angriffspfade Sie zuerst absichern sollten?

Die meisten mit dem Schutz von IT-Netzwerken betrauten Personen stützen sich auf Listen und prüfen Tausende allgemeine Konfigurationsprobleme. Angreifer hingegen stützen sich oft auf Diagramme, um schneller einen Weg in die Steuerungsebene oder zu den Tier-0-Assets eines Unternehmens zu finden. Hier kommt SpecterOps BloodHound Enterprise ins Spiel.

Mit der AD-Sicherheitsbewertung von BloodHound Enterprise können wir wichtige Einblicke in die Sicherheit Ihrer hybriden AD-Umgebung liefern und Ihnen Ihre kritischsten Assets in AD und Azure (Azure AD und Azure Resource Manager) aufzeigen – also die Ressourcen, über die Angreifer auf keinen Fall die Kontrolle erlangen dürfen. Mit der Active Directory-Sicherheitsbewertung werden die potenziellen Pfade, über die ein Angreifer sich Zugriff auf die wichtigsten Ressourcen in Ihrer Umgebung verschaffen könnte, visuell dargestellt.



Identifizieren und quantifizieren sie die Problemstellen, die die meisten Angriffspfade für Ihre kritischen Assets eliminieren.

Finden und beseitigen Sie die Problemstellen – die übergeordneten Angriffspfade – und verbessern Sie so effektiv Ihren Sicherheitsstatus.

Funktionsweise

Zuerst berät sich einer unserer erfahrenen Lösungsarchitekten mit Ihrem Team, um BloodHound Enterprise einzurichten und einen anfänglichen Scan Ihrer Umgebung durchzuführen. Dann zeigen wir Ihnen jeden möglichen Weg zu Ihren Tier-0-Assets und ermitteln jede Beziehung in Ihrer Hybrid-Umgebung, die ein Angreifer missbrauchen könnte, um sich Zugriff zu verschaffen. Mit BloodHound Enterprise analysieren wir jeden Angriffspfad und die zugehörigen Problemstellen auf diesen Angriffspfaden, um Ihnen einen Überblick

Vorteile:

- Analysiert die Auswirkungen jedes beliebigen Punkts in einem Angriffspfad
- Identifiziert den optimalen Ort zum Blockieren der größtmöglichen Anzahl von Pfaden
- Ordnet die endliche Menge an Problemstellen nach kollektiver Risikoreduzierung
- Minimiert den Korrekturaufwand und eliminiert die nachträgliche Bereinigung von Fehlkonfigurationen

über das Risiko zu geben, dem Ihr Unternehmen mit Ihrer hybriden AD-Umgebung ausgesetzt ist. Wenn Sie Ihre Angriffspfad-Verwaltung durch Eliminierung dieser Problemstellen verbessern, optimieren Sie damit auch Ihren Sicherheitsstatus insgesamt.

Kontinuierliche Bewertung

Unternehmensnetzwerke, Benutzerberechtigungen, Anwendungsberechtigungen und die Mitgliedschaften in Sicherheitsgruppen sind dynamisch. Immer wenn sich ein privilegierter Benutzer bei einem System anmeldet, hinterlässt er Tokens und Anmeldeinformationen, die Angreifer zu stehlen versuchen können. Die Verbindungen und Verhaltensweisen, aus denen sich Angriffspfade zusammensetzen, verändern sich kontinuierlich und deshalb müssen auch die Angriffspfade selbst kontinuierlich aufs Neue nachvollzogen werden. BloodHound Enterprise deckt folgende Aspekte fortlaufend ab:

- Grafische Darstellung sämtlicher Beziehungen und Verbindungen
- Umfassender Überblick über die realen Berechtigungen
- Aufdeckung neuer und bestehender verborgener Angriffspfade in AD und Azure AD
- Sicherstellen, dass Ihr Team die ständigen Sicherheitsanforderungen Ihres Unternehmens erfüllt

Schwerpunktbereiche

Die AD-Sicherheitsbewertung liefert Ihnen Folgendes:

- Praktische Bereinigungen ohne drastische Änderungen an AD/Azure AD oder negative Auswirkungen
- Präzise und umfassende Informationen zur Eliminierung von Angriffspfaden
- Anweisungen zum Bestätigen, dass zu entfernende Berechtigungen auch wirklich nicht benötigt werden
- Transparenz mit Blick auf alle AD-Angriffspfade
    - Auflistung und Identifizierung aller Angriffspfade, die Angreifern für die laterale Bewegung und Rechteausweitung zur Verfügung stehen
- Priorisierung von Problemstellen mit praktischen Bereinigungen
    - Vorschläge zum Beseitigen von Millionen von Angriffspfaden mit minimalem Aufwand und Informationen zur Umsetzung in Ihrer AD-Architektur
- Analyse der Verbesserung Ihres AD-Sicherheitsstatus im Laufe der Zeit
- Ermittlung des Gefährdungsniveaus Ihrer kritischen Ziele und Nachverfolgung der Effektivität von Bereinigungen

Nächste Schritte

SpecterOps BloodHound Enterprise hilft Ihnen zwar beim Abbilden und Identifizieren der Angriffspfade und Problemstellen in Ihrer hybriden AD-Umgebung, es liegt aber an Ihnen, die ermittelten Problemstellen zu beseitigen und Parameter zum Gewährleisten der fortlaufenden Sicherheit Ihrer Umgebung einzurichten. Aber auch hier kann Quest Ihnen behilflich sein.

Umfassende Risikobewertung und Bedrohungsüberwachung

Kombinieren Sie SpecterOps BloodHound Enterprise mit Change Auditor und On Demand Audit, um eine umfassende Lösung zur Risikobewertung und Bedrohungsüberwachung zu erhalten. Mit diesen Komponenten können Sie sämtliche Sicherheitsänderungen in Ihren AD und Azure AD-Umgebungen umfassend auditieren, einschließlich Änderungen auf Benutzer- und Gruppenebene. Außerdem sind Sie imstande, Exploits wie die Exfiltrierung der AD-Datenbank durch Offline-Kopie oder nicht autorisierte Domänenreplikation frühzeitig zu erkennen. Ebenso sind Sie in der Lage, den Zugriff von Angreifern auf Pfade zu blockieren – einschließlich privilegierter Gruppen, GPOs und Exfiltrierung Ihrer AD-Datenbank – und so kostspielige Ransomware-Angriffe einzudämmen oder zu vermeiden.

Verringerung von Angriffspfaden mit abgesicherten GPOs

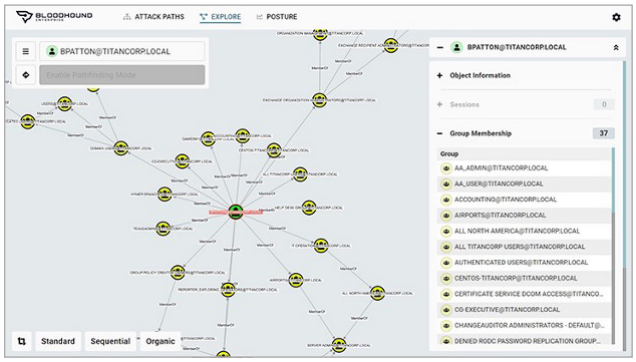
Bei Kombination von SpecterOps BloodHound Enterprise mit GPOADmin können Sie die Angriffspfad-Verwaltung durch Absicherung von GPOs effektiv verbessern. Mit diesen Lösungen können Sie bereits vor der Bereitstellung sicherstellen, dass jegliche Änderungen den Best Practices der Änderungsverwaltung entsprechen. Dies ist ein wichtiger Schritt bei der Verwaltung von Active Directory-Gruppenrichtlinien. Außerdem können Sie GPOs kontinuierlich durch automatisierte Attestierung validieren – dies ist für jede Drittanbieterlösung zur Verwaltung von Gruppenrichtlinien unerlässlich. Falls eine GPO-Änderung unerwünschte Auswirkungen hat, können Sie schnell wieder auf eine funktionierende GPO umstellen, damit Ihre Umgebung in Sekundenschnelle wieder reibungslos läuft.

Risikoschutz und sichere Bereinigung

Für echten Risikoschutz und eine sichere Bereinigung empfiehlt sich die Kombination von SpecterOps BloodHound Enterprise mit Recovery Manager for Active Directory Disaster Recovery Edition und On Demand Recovery. Mit dieser Produktkombination verfügen Sie über umfassende Funktionen zur Sicherung Ihres hybriden Active Directory und schnellen Wiederherstellung bei Fehlern, Beschädigung oder Notfällen. Außerdem können Sie jegliche Änderungen seit der letzten Sicherung identifizieren, indem Sie den Onlinestatus von AD mit seiner Sicherung (oder mehreren Sicherungen) vergleichen. Sie können jedes beliebige AD-Objekt wiederherstellen, einschließlich Benutzern, Attributen, Organisationseinheiten (OUs), Computern, Subnetzen, Standorten, Konfigurationen und Gruppenrichtlinienobjekten (GPOs).

Über Quest

Quest stellt Softwarelösungen bereit, mit denen das Potenzial neuer Technologien in einer immer komplexeren IT-Landschaft ausgeschöpft werden kann. Von der Datenbank- und Systemverwaltung über die Verwaltung von Active Directory und Office 365 bis hin zur Cyber Resilience: Quest hilft Kunden, bereits heute die IT-Herausforderungen von morgen zu bewältigen. Quest Software: Where Next Meets Now.



Visualisieren Sie die komplexen Verbindungen und Beziehungen in AD und Azure, um nachvollziehen zu können, wo Fehlkonfigurationen zu Risiken für die wichtigsten Assets Ihres Unternehmens führen.

SYSTEMANFORDERUNGEN

System

- Windows Server 2012+
- 16 GB RAM
- 100 MB Speicherplatz
- .NET 4.5.2+

Netzwerktechnologie

- TLS an 443/TCP für Ihre Tenant-URL (vom Account-Team bereitgestellt)
- TLS an 443/TCP für den Azure-Tenant (sofern zutreffend)

Berechtigungen

SharpHound (On-Premises-Active Directory-Sammlung)

- Dienstkonto zur lokalen Administratorgruppe hinzugefügt

AzureHound (Azure-Sammlung)

- Directory Reader für Azure AD-Tenants
- Reader für alle Azure Abonnements
- Microsoft Graph
  - AppRoleAssignment.ReadWrite.All
  - RoleManagement.Read.All