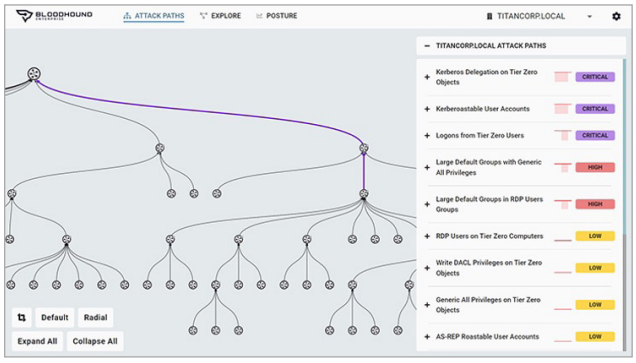
Évaluation de la sécurité d'Active Directory

Limitez les voies d'attaque et sécurisez Active Directory et Azure avec SpecterOps BloodHound Enterprise

L'un des aspects essentiels de la protection d'Active Directory (AD) et d'Azure contre les cyberattaques est d'identifier et de sécuriser les voies d'attaque que les pirates pourraient utiliser pour infiltrer votre environnement AD. Et cela n'est pas surprenant, puisque plus de 95 millions de comptes utilisateur AD subissent des attaques chaque jour. Mais comment choisir quelles voies d'attaque sécuriser en priorité ?

Alors que la plupart des personnes chargées de défendre les réseaux informatiques pensent en termes de listes et vérifient des milliers de problèmes de configuration génériques, les pirates pensent souvent en termes de graphiques, ce qui leur permet de trouver plus rapidement un chemin vers le plan de contrôle d'une organisation ou ses actifs de niveau zéro. C'est là que SpecterOps BloodHound Enterprise entre en jeu.

Notre évaluation de la sécurité d'AD repose sur BloodHound Enterprise. Nous sommes donc en mesure de vous fournir des informations essentielles sur la sécurité de votre environnement AD hybride en vous montrant un sur-ensemble de vos actifs stratégiques dans AD et Azure (Azure AD et Azure Resource Manager) : les actifs qui seraient responsables de votre perte si un cybercriminel venait à mettre la main dessus. Avec l'évaluation de la sécurité d'Active Directory, vous verrez les chemins potentiels qu'un pirate pourrait emprunter pour accéder aux ressources les plus précieuses de votre environnement.



Identifiez et quantifiez les points d'étranglement des voies d'attaque qui permettront d'éliminer le plus de chemins vers vos actifs stratégiques.

Trouvez et supprimez les points d'étranglement, les voies d'attaque principales, pour améliorer votre politique de sécurité.

Comment cela fonctionne-t-il ?

L'un de nos architectes de solutions expérimentés commence par consulter votre équipe pour configurer BloodHound Enterprise et effectue l'analyse initiale de votre environnement. Ensuite, nous vous aidons à identifier tous les chemins possibles vers vos actifs de niveau zéro et toutes les relations dans votre environnement hybride qu'un pirate pourrait exploiter pour accéder à vos données. Avec BloodHound Enterprise, nous mesurons chaque voie d'attaque, ainsi que les points d'étranglement correspondants sur ces chemins. Cela vous donne une vue générale des risques qui existent pour l'organisation au niveau de votre environnement AD hybride. En améliorant la gestion des voies

Avantages :

- Mesure l'impact de tous les points d'une voie d'attaque
- Identifie l'emplacement optimal qui permet de bloquer le plus grand nombre de chemins
- Classe cet ensemble fini de points d'étranglement par réduction des risques collectifs
- Réduit les efforts de correction et élimine le nettoyage de la dette due aux mauvaises configurations

d'attaque avec l'élimination de ces points d'étranglement, vous pouvez également constater l'effet de ces changements sur votre politique de sécurité globale.

Évaluation continue

Les réseaux d'entreprise, les privilèges utilisateur, les autorisations des applications et les appartenances aux groupes de sécurité sont des éléments dynamiques. Chaque fois qu'un utilisateur à privilèges accède à un système, il laisse derrière lui des jetons et des informations d'identification que vos adversaires peuvent essayer d'obtenir. Les connexions et comportements des voies d'attaque évoluent continuellement. Par conséquent, ces chemins eux-mêmes doivent être mappés en continu. Avec BloodHound Enterprise, vous pouvez profiter de ces fonctionnalités en continu :

- Graphiques de chaque relation et connexion
- Compréhension complète des autorisations réelles
- Présentation des voies d'attaque cachées, nouvelles et existantes, dans AD et Azure AD
- Garantie que votre équipe répond aux besoins de sécurité continus de votre organisation

Domaines d'intervention

Avantages de l'évaluation de la sécurité d'AD :

- Corrections pratiques sans modification drastique ni impact négatif sur AD/Azure AD
- Recommandations précises et complètes pour vous aider à éliminer les voies d'attaque
- Instructions pour savoir comment vérifier que les privilèges supprimés ne sont pas requis
- Visibilité sur toutes les voies d'attaque AD
    - Énumération et détection de toutes les voies d'attaque accessibles aux pirates : mouvement latéral et escalade des privilèges
- Priorisation des points d'étranglement avec des corrections pratiques
    - Identification de la méthode de suppression de millions de voies d'attaque avec des efforts minimum, et ce, dans votre architecture AD existante
- Mesure des améliorations de votre politique de sécurité AD au fil du temps
- Identification du niveau d'exposition des cibles à forte valeur et suivi de l'efficacité des corrections

Étapes suivantes

Alors que SpecterOps BloodHound Enterprise vous permet de cartographier et d'identifier les voies d'attaque et points d'étranglement de votre environnement AD hybride, c'est à vous d'éliminer les goulots d'étranglement identifiés et de définir des paramètres pour garantir la sécurité continue de votre environnement. Quest peut vous aider.

Solution complète d'évaluation des risques et de surveillance des menaces

Associez SpecterOps BloodHound Enterprise avec Change Auditor et On Demand Audit pour profiter d'une solution complète d'évaluation des risques et de surveillance des menaces. Vous pourrez réaliser un audit complet de toutes les modifications de sécurité apportées à vos environnements AD et Azure AD, y compris au niveau des utilisateurs et des groupes, et détecter rapidement les exploits comme l'exfiltration de la base de données AD via une copie hors ligne ou une réplication de domaine non autorisée. Vous allez aussi pouvoir bloquer l'accès des pirates aux voies d'attaques : groupes à privilèges, objets de stratégie de groupe et exfiltration de votre base de données AD pour limiter et éviter des attaques par rançongiciel coûteuses.

Élimination des voies d'attaque via la sécurisation des objets de stratégie de groupe

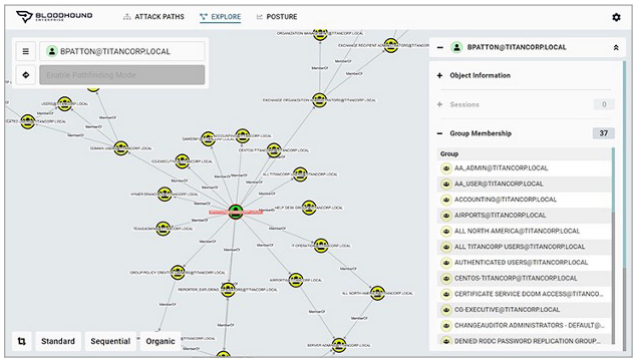
En utilisant SpecterOps BloodHound Enterprise avec GPOADmin, vous pouvez améliorer la gestion des voies d'attaque en sécurisant les objets de stratégie de groupe. Ces solutions vous permettent de garantir que les modifications respectent les bonnes pratiques de gestion des modifications avant le déploiement, une étape critique de la gestion des stratégies de groupe Active Directory. De plus, vous pouvez valider continuellement les GPO au moyen d'une attestation automatisée, une nécessité pour toute solution de gestion des stratégies de groupe tierces. De même, vous pouvez rapidement revenir à un GPO fonctionnel si une modification avait un effet indésirable. Ainsi, votre environnement peut être de nouveau opérationnel en quelques secondes.

Protection contre les risques et garantie des corrections

Pour une véritable protection contre les risques et la garantie des corrections, associez SpecterOps BloodHound Enterprise avec Recovery Manager for Active Directory Disaster Recovery Edition et On Demand Recovery. Cette combinaison de produits vous offre des fonctionnalités complètes pour la sauvegarde d'Active Directory hybride et la restauration rapide en cas d'erreur, de corruption ou d'incident. De plus, vous pouvez identifier les modifications effectuées depuis la dernière sauvegarde, en comparant l'état en ligne d'AD avec sa sauvegarde ou en comparant plusieurs sauvegardes. Vous avez également la possibilité de restaurer tous types d'objets dans l'environnement AD, notamment des utilisateurs, des attributs, des unités organisationnelles, des ordinateurs, des sous-réseaux, des sites, des configurations et des objets de la politique par groupe.

Profil de Quest

Quest crée des solutions logicielles conçues pour exploiter tous les avantages des nouvelles technologies dans un paysage informatique toujours plus complexe. De la gestion des bases de données et des systèmes à la gestion d'Active Directory et Office 365, en passant par la cybersécurité et la résilience, Quest aide ses clients à relever leurs prochains défis informatiques dès à présent. Quest Software. Où demain rencontre aujourd'hui.



Visualisez les connexions et relations complexes dans AD et Azure pour comprendre où les mauvaises configurations ont exposé les actifs les plus précieux de votre organisation.

CONFIGURATION REQUISE

Système

- Windows Server 2012+
- 16 Go de mémoire RAM
- 100 Go d'espace sur le disque dur
- .NET 4.5.2+

Réseau

- TLS sur 443/TCP vers l'URL de votre tenant (fourni par votre équipe de compte)
- TLS sur 443/TCP vers le tenant Azure (le cas échéant)

Autorisations

SharpHound (collection Active Directory sur site)

- Compte de service ajouté au groupe d'administrateurs local

AzureHound (collection Azure)

- Directory Reader sur le tenant Azure AD
- Reader sur tous les abonnements Azure
- Microsoft Graph
  - AppRoleAssignment.ReadWrite.All
  - RoleManagement.Read.All