SentinelOne

Singularity | RANGER. AD Assessor

Checklist pour protéger Active Directory

Compte tenu de leur intérêt accru pour les surfaces d'attaque axées sur les identités, les cybercriminels ciblent en priorité les environnements Active Directory sur site et hébergés dans le cloud. De leur côté, les administrateurs Active Directory doivent trouver un équilibre entre exigences opérationnelles et mesures de sécurité restrictives, ce qui rend la protection de ces environnements particulièrement complexe.

Si la plupart des solutions sont en mesure de protéger les infrastructures sur site et Azure AD, les professionnels de sécurité peinent à trouver la solution adaptée au profil de risque propre à leur entreprise.

Les équipes de sécurité peuvent utiliser la checklist suivante pour évaluer les risques et les vulnérabilités de leurs procédures de sécurité Active Directory.

Questions d'évaluation de la protection d'Active Directory

Critères de cyberhygiène pour les environnements Active Directory sur site et dans le cloud

- Disposez-vous d'un inventaire de l'ensemble des comptes utilisateur ou équipement ?
- Disposez-vous d'un inventaire de l'ensemble des privilèges et droits d'accès pour chaque compte ?
- Avez-vous implémenté le concept du moindre privilège pour tous les comptes ?
- Les paramètres de sécurité d'Active Directory sont-ils régulièrement vérifiés et évalués ?
- Les vulnérabilités Kerberos sont-elles régulièrement évaluées dans Active Directory ?
- Les serveurs Active Directory sont-ils prémunis contre les dernières CVE et autres vulnérabilités ?
- Les relations d'approbation entre les forêts sont-elles régulièrement auditées ?

Critères d'identification des indicateurs d'attaque

- Les tentatives de collecte de données Active Directory sont-elles détectées et bloquées ?
- Des stratégies d'audit sont-elles appliquées ?
- Les journaux d'audit sont-ils périodiquement analysés ?
- Disposez-vous d'une visibilité sur la duplication des annuaires de domaine ?
- Disposez-vous d'une visibilité sur les tentatives de découverte des autorisations au niveau des utilisateurs et des groupes ?
- Disposez-vous d'une visibilité en temps réel sur les modifications en masse dans Active Directory ?
- Disposez-vous d'une détection en temps réel des attaques, telles que les attaques Kerberoasting et DCShadow ?