

Quest Security Guardian

Gardez une longueur d'avance sur les cyberattaques ciblant Active Directory grâce à une solution de sécurité AD qui révèle ce qui s'est passé, ce qui a été exposé et comment résoudre le problème.

Quest Security Guardian est un outil de sécurité Active Directory conçu pour réduire votre surface d'attaque. À partir d'un espace de travail simplifié et unifié, Security Guardian filtre efficacement les alertes en donnant la priorité aux vulnérabilités les plus exploitables et aux configurations Active Directory qui requièrent une attention particulière. La solution met en évidence ce qui s'est passé, si vous êtes exposé et comment résoudre le problème.

Protégez vos assets critiques Tiers Zero grâce aux capacités suivantes :

- Comparer la configuration actuelle d'Active Directory aux bonnes pratiques du secteur
- Verrouiller les objets critiques, y compris les GPO, contre les erreurs de configuration et les compromissions
- Surveiller en continu les indicateurs d'exposition et de compromission pour garder une longueur d'avance sur les menaces

La sécurité de l'identité, en particulier d'Active Directory (AD), est essentielle pour éviter toute interruption dans l'activité de votre organisation. Les conséquences des arrêts de service d'AD sont désastreuses, avec des

coûts astronomiques pouvant atteindre 730 000 dollars par heure, selon le cabinet Forrester. De plus, si l'on considère que 80 % des violations impliquent désormais l'utilisation d'identités compromises, AD est devenu une cible de choix. Quest Security Guardian vous aidera à réduire la surface d'attaque de votre AD simplement et rapidement.

Évaluation de la sécurité d'AD

Comparez la configuration actuelle d'Active Directory aux bonnes pratiques prédéfinies du secteur. Vous disposerez d'une visibilité totale sur les indicateurs d'exposition, les indicateurs de compromission et les assets Tiers Zéro. Cet outil de sécurité Active Directory permet non seulement d'atténuer les menaces, mais aussi de réduire la surface d'attaque.

Avantages :

- Réduire la surface d'attaque en évaluant votre AD par rapport aux meilleures pratiques du secteur
- Simplifier la sécurité AD avec une visibilité, une protection et un contrôle complets des assets critiques
- Atténuer les écarts de configuration d'AD et garder une longueur d'avance sur les attaques
- Limiter le nombre d'alertes et identifier les menaces réelles en se concentrant sur les alertes importantes
- Mettre les indicateurs d'exposition et de compromission en corrélation afin de réagir rapidement contre les menaces



Priorité donnée aux assets stratégiques

Identifiez et hiérarchisez les assets Tiers Zéro sans effort, en veillant à ce que les plus faciles à attaquer reçoivent la plus grande attention. Prenez le contrôle de ces assets critiques, vous pourrez alors modifier la liste des objets Tiers Zéro afin de rester en phase avec le niveau de sécurité de votre organisation.

Prévention des menaces AD

Sécurisez les objets AD stratégiques contre la compromission et les mauvaises configurations, y compris les GPO sensibles. Cet outil de sécurité Active Directory fournit des rapports ciblés sur l'état des objets, vous donnant le contexte nécessaire pour prendre les mesures appropriées.

Détection des menaces AD

Gardez le cap sur vos objectifs de réduction des menaces en utilisant Security Guardian pour surveiller en continu les indicateurs de compromission et les écarts de configuration, afin d'être bien préparé pour répondre rapidement aux incidents de sécurité potentiels.

Réponse rapide aux incidents

En cas d'activité suspecte, répondez aux questions « qui, quoi, où, comment, quand » grâce à des notifications intelligentes et contextuelles qui contribueront à réduire le nombre d'alertes parasites. Transmettez facilement les indicateurs d'exposition et les indicateurs de compromission à vos outils SIEM, tels que Microsoft Sentinel et Splunk, pour une intégration transparente et une visibilité centralisée.

Espace de travail de sécurité AD unifié

Concentrez-vous sur les opérations primordiales grâce à une interface conviviale qui offre une visibilité sur les indicateurs d'exposition, les indicateurs de compromission et d'autres signaux de sécurité de manière transparente.

“ La reconstruction d'un objet AD qui n'a pas été modifié correctement peut prendre des heures et avoir ainsi un impact sur les opérations (...). La protection des objets par Quest nous permet d'éviter ces problèmes. ”

Alessandro Bottin, Responsable des infrastructures et des opérations mondiales, Prysmian Group

Profil de Quest

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