

Cyber Résilience Active Directory Hybride

Protégez votre environnement AD hybride et atténuez les risques en implémentant le framework NIST.

L'Active Directory (AD) est le pilier de votre organisation, mais c'est également la cible préférée de tous les cybercriminels. En effet, s'ils peuvent contrôler votre AD, ils peuvent contrôler votre entreprise entière. Mais la constante évolution et la complexité des environnements AD, notamment s'ils sont hybrides, rendent leur sécurisation très difficile. Les ransomwares, les menaces internes, les mauvaises configurations - un faux pas et les adversaires ont un pied dans la porte.

En 2021, 25 milliards d'attaques ont été signalées sur les comptes Azure AD. Sans un cadre complet de cyber résilience AD et AAD en place, votre organisation sera victime de menaces très réelles.

Pour combattre les menaces avancées et évolutives d'aujourd'hui, vous avez besoin d'une défense en multi niveaux qui vous protège contre chaque phase du cycle de vie d'une attaque. Chez Quest, nous proposons une approche qui aborde la défense en profondeur à chaque niveau du framework NIST, afin que vous puissiez atténuer les risques avant, pendant et après une attaque.

Les solutions de notre suite de cyber résilience pour l'AD hybride travaillent main dans la main et se complètent les unes les autres pour vous donner la possibilité de :



Identifier les indicateurs d'exposition (IOEs) et prioriser les chemins d'attaque qu'un adversaire pourrait emprunter pour compromettre votre environnement.



Protéger votre environnement pour empêcher les attaquants de modifier des objets critiques, paramètres de GPO ou de capturer votre base de données AD pour voler des informations d'identification.



Détecter les indicateurs de compromission (IOCs) avec une surveillance et des alertes en temps réel ainsi qu'une détection d'anomalies d'activité.



Répondre aux menaces et rassembler rapidement des informations pour accélérer les investigations forensiques.



Restaurer AD en toute sécurité après une attaque, aboutie ou non, ou un désastre quel qu'il soit le plus rapidement possible afin que l'organisation puisse recommencer à travailler en minimisant au maximum les impacts.



Comment Quest peut vous aider

Quest se différencie en proposant un cycle de vie complet et continu de la cyber résilience AD qui offre une défense en profondeur à travers les différents niveaux correspondant au framework de cybersécurité NIST.

Quest AD Risk Assessment Suite

Produits inclus : SpecterOps BloodHound Enterprise, Quest Change Auditor et Quest On Demand Audit



- Évaluez et priorisez les chemins d'attaque dans vos environnements pour éliminer ceux qui présentent le plus d'exposition et les risques les plus importants.
- Auditez tous les changements de sécurité AD et Azure AD pour détecter les menaces le plus tôt possible, y compris la réplication de domaines non autorisée, l'extraction hors ligne de la base NTDS.dit et les actions suspectes sur l'annuaire, le DNS ou encore les GPO.
- Bloquez les actions des attaquants telles que les modifications de groupes, d'objets critiques, de GPOs, ou encore la capture offline de votre base de données AD.

Quest AD Risk Protection Suite

Produits inclus : Quest AD Risk Assessment Suite + Quest GPOADmin



- Assurez-vous que les modifications de GPO respectent les meilleures pratiques de gestion des changements avant déploiement.
- Validez continuellement les GPOs à travers un processus de validation et d'attestation automatisé.
- Améliorez l'audit des GPO et vérifiez la cohérence des paramètres en comparant les différentes versions de GPO entre elles via une gestion historique des versions automatisée.
- Revenez rapidement à une version fonctionnelle d'une GPO en cas d'effet indésirable d'un changement.

Quest Hybrid AD Cyber Resiliency Suite

Produits inclus : Quest AD Risk Protection Suite + Quest Recovery Manager Disaster Recovery Edition et Quest On Demand Recovery

- Automatisez l'ensemble des étapes de la procédure de restauration de forêt AD.
- Protégez les sauvegardes AD des compromissions et éliminez le risque de réinfection par des malwares.
- Restaurez les objets purement cloud tels que les Service Principals, les règles d'accès conditionnelles, les groupes Microsoft 365 etc...



A propos de Quest

Quest crée des solutions logicielles qui permettent de tirer parti des avantages des nouvelles technologies dans un paysage informatique de plus en plus complexe. De la gestion de bases de données et des systèmes, à la gestion d'Active Directory et d'Office 365 et la résilience en cybersécurité, Quest aide les clients à résoudre leur prochain défi informatique maintenant. Quest Software. Quand le futur se rencontre aujourd'hui.