Biotechnologie

Étude de cas

CYBER RÉSILIENCE

UTILISATION DE LA GESTION DES IDENTITÉS

À PROPOS DU CLIENT

Une entreprise biopharmaceutique/biotechnologique de premier plan avec une présence mondiale et ayant des exigences de conformité pour la protection des processus PII, IP et GxP.

OBJECTIFS

Le client souhaitait réduire l'exposition aux attaques pour les mouvements latéraux ainsi que les escalades privilégiées.

En outre, réduisez les fuites volontaires/involontaires d'informations d'identification endes employés qui perturberaient ou compromettraient les processus de fabrication.

Le client recherchait une solution qui facilite l'utilisation pour les utilisateurs non informaticiens et fournit suffisamment d'outils pour le libre-service.

APPROCHER

ISSQUARED® a mené divers ateliers avec le client pour discuter des options et stratégies les plus fiables. En conséquence, nous avons décidé que la meilleure approche serait d'empêcher l'utilisateur d'utiliser le même mot de passe sur plusieurs comptes dans différents domaines Active Directory non approuvés (chaque individu en a au moins deux). Les éléments suivants ont été les moteurs de la conception de la solution :

a) Restreindre l'exposition des informations d'identification privilégiées dans le réseau d'entreprise.

b) Politique d'identification stricte pour les comptes privilégiés.

c) Non perturbateur pour le personnel non informatique dans l'exercice de ses fonctions quotidiennes.

d) ré. Options et notifications en libre-service pour les utilisateurs pour toutes les actions correctives attribuées.

e) Intégration et provisionnement automatisés pour les utilisateurs migrés avec activation en libre-service.

f) Mesures pour évaluer l'efficacité.

SOLUTION

COMPTES ADMINISTRATEUR/UTILISATEUR PRIVILÉGIÉ

Une solution de sauvegarde des mots de passe (PI) de pointe a été déployée sur tous les sites. L'équipe ISSQUARED® a mis en place un changement de mot de passe quotidien et un processus d'enregistrement/de départ. Ces mots de passe ont été générés aléatoirement par le système assurant l'absence de conflit avec d'autres comptes appartenant au même utilisateur.

Le libre-service a été fourni sur la plate-forme de stockage des mots de passe pour que les utilisateurs administrateurs déverrouillent leurs comptes administrateurs en cas de verrouillage de compte.

Un outil de gestion des journaux et de notification d'événements a également été configuré pour suivre et signaler les demandes de changement de mot de passe fréquentes, maintenir une piste d'audit de toutes les extractions de compte.

L'exposition aux comptes privilégiés dans le réseau de l'entreprise a été encore réduite en configurant de nouveaux hôtes bastions avec accès uniquement aux comptes réguliers.

COMPTES D'UTILISATEURS RÉGULIERS

Le provisionnement des utilisateurs migrés a été effectué automatiquement par ORSUSTM Identity Access & Governance.

L'accès à toutes les applications migrées a été restauré automatiquement.

Une option de libre-service sous la forme d'ORSUSTM Identity Access & Governance a été fournie aux utilisateurs finaux pour répondre activement aux demandes de changement de mot de passe et gérer leur compte régulier en général.

Des coffres-forts de mots de passe statiques ont été fournis aux utilisateurs de la solution BeyondTrust pour gérer les mots de passe des comptes réguliers.

Étant donné que la plupart des utilisateurs non-administrateurs n'étaient pas du personnel informatique, il a été décidé de s'appuyer sur un processus d'escalade via des notifications par courrier électronique aux responsables respectifs en cas de mots de passe non conformes.

Les métriques sont partagées mensuellement avec la direction pour une escalade supplémentaire sur les défaillants.

RÉSULTATS

L'exposition à 0 % des comptes privilégiés non fiables renforce la sécurité contre les attaques de mouvement latéral.

0% de correspondance de mot de passe pour les comptes d'administrateur et d'utilisateur standard protège contre les attaques par escalade de privilèges.

~ 80% de réduction des conflits de mots de passe pour les comptes réguliers.

Migration accélérée des applications LoB vers des domaines isolés permettant de réduire l'exposition aux processus métier critiques.

Adoption à 100 % par les utilisateurs d'outils en libre-service facilitant la sécurité et la facilité d'utilisation.

ISSQUARED®

HQ: 2659 Townsgate Rd, Suite 227
Westlake Village CA 91361 USA

+1 805 371 0585
+1 800 779 0587

support@issquaredinc.com
www.issquaredinc.com