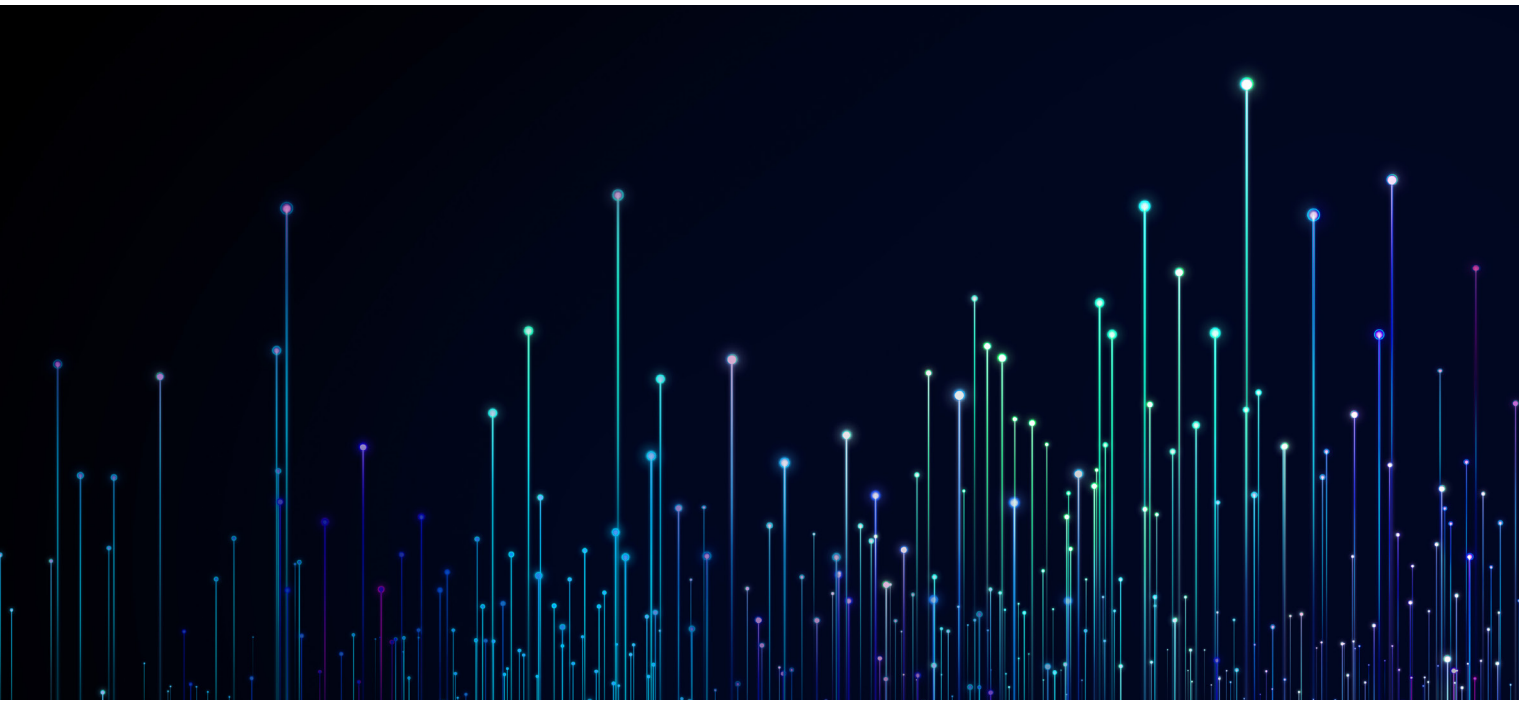
Top 10 des rapports et alertes de sécurité Active Directory dont vous avez besoin

Renforcez votre cyber-résilience et détectez les menaces actives avec Change Auditor de Quest.



INTRODUCTION

La défense du périmètre traditionnel ne suffit plus. Aujourd'hui, les identités constituent un nouveau périmètre : les pirates ciblent activement les comptes de vos utilisateurs et utilisent des informations d'identification compromises pour causer des ravages au sein de votre réseau. Dans les faits, Microsoft rapporte que 95 millions de comptes AD sont la cible de cyberattaques chaque jour et que 1,2 million de comptes Azure AD sont compromis chaque mois. Sans oublier les risques associés aux salariés malveillants et aux travailleurs stressés et distraits. Il est donc évident que chaque entreprise doit mettre la priorité sur la détection des menaces au sein de l'environnement IT.

Qu'est-ce que cela signifie exactement ? Les experts en sécurité recommandent d'adopter une approche qui suppose nécessairement une violation : vous devez considérer que certains comptes sont déjà compromis et que des salariés malveillants opèrent dans votre environnement IT, ce qui vous oblige à mener des audits de sécurité internes renforcés pour protéger votre ressource la plus stratégique et la plus ciblée : Active Directory. AD est l'épine dorsale de votre organisation, fournissant l'authentification et l'autorisation pour chaque ressource critique dans votre environnement. Par conséquent, vous ne devez pas gérer AD en tant que simple infrastructure, mais en tant que ressource de sécurité.

Change Auditor de Quest est l'une des plus puissantes solutions dont vous pouvez équiper votre arsenal de sécurité. Dans le monde actuel en rapide évolution, vous ne pouvez tout simplement pas passer des heures à décortiquer les logs d'audit d'AD ni courir le risque de manquer des événements critiques parmi la multitude de résultats ou de ne pas réussir à identifier un schéma d'événements indiquant une attaque. Avec les fonctions d'audit en temps réel de Change Auditor, vous savez immédiatement ce qu'il se passe dans votre environnement, ce qui vous permet d'économiser un temps précieux tout en renforçant votre sécurité et en assurant la conformité aux normes en vigueur. Mieux encore, Change Auditor vous permet également d'effectuer des recherches et de les transformer en alertes et rapports utiles et pertinents, le tout depuis une seule et même console centrale.

Ce livre blanc dévoile les 10 principaux rapports et alertes dont vous avez besoin pour assurer la stabilité et la sécurité de votre environnement Active Directory, et explique comment les obtenir facilement avec Change Auditor.

Une seule modification inappropriée d'un GPO peut avoir de sévères répercussions. Recevez immédiatement des alertes sur les événements critiques avec Change Auditor.

DIX PRINCIPAUX RAPPORTS ET ALERTES DE CHANGE AUDITOR

1. Modifications d'une politique par groupe

Les objets de la politique par groupe (GPO) comptent parmi les éléments les plus stratégiques de votre infrastructure. Une seule modification inappropriée d'un GPO peut entraîner une énorme faille dans votre politique de sécurité, permettant par exemple à des utilisateurs (ou à des pirates ou des logiciels malveillants utilisant des informations d'identification volées) de copier des données sur des clés USB, d'utiliser une invite de commande puissante ou d'installer des applications indésirables.

Les logs d'événements natifs consignent les modifications d'un GPO, mais ne capturent pas les paramètres spécifiques qui ont été modifiés. Par conséquent, le processus permettant d'isoler et de corriger un problème est chronophage et propice aux erreurs, ce qui rend votre entreprise vulnérable pendant une plus longue période.

Change Auditor ne s'appuie pas uniquement sur des logs natifs et peut ainsi fournir des détails complets sur les modifications apportées à vos GPO, notamment les paramètres, l'héritage, les liens et l'état général. De plus, contrairement aux outils d'audit natifs, Change Auditor affiche tous les événements de modification, dont les modifications des GPO, dans un format standardisé et pertinent qui inclut les réponses à cinq questions clés ainsi que les valeurs avant/après essentielles :

- Qui a effectué la modification
- Quel objet a été modifié
- Quand l'objet a été modifié
- Où a eu lieu la modification
- Station de travail source

Ces informations cohérentes et détaillées vous permettent d'identifier rapidement toute modification indésirable ou non autorisée apportée à vos GPO, et de l'annuler avant qu'elle n'entraîne des dommages au sein de votre entreprise.

En outre, Change Auditor ne fournit pas seulement des rapports clairs, mais envoie aussi des alertes en temps réel pour toutes les modifications de votre choix. Vous pouvez notamment recevoir des notifications proactives au sujet de modifications apportées à vos GPO les plus importants, comme ceux qui gouvernent votre stratégie de mot de passe ou votre stratégie de verrouillage

Figure 1 : Change Auditor affiche les cinq éléments clés de chaque modification ainsi que les valeurs avant/après indispensables.

de comptes, pour vous permettre de réagir immédiatement. Mieux encore, Change Auditor peut empêcher n'importe quel utilisateur de modifier des objets Active Directory critiques, comme les GPO, dans un premier temps, qu'il s'agisse d'un administrateur maladroit ou peu expérimenté, ou d'un pirate utilisant des informations d'identification volées.

Si vous avez besoin d'une gouvernance complète de vos GPO, renseignez-vous sur GPOADmin, qui offre davantage de fonctionnalités, notamment le contrôle d'accès basé sur les rôles (RBAC), la délégation, l'historique des versions, les workflows d'approbation, les déploiements planifiés et des fonctions complètes de restauration.

2. Verrouillages de comptes d'utilisateur

Les verrouillages de comptes d'utilisateur n'engendrent pas uniquement une grande frustration chez les utilisateurs, ils peuvent interrompre brusquement des processus stratégiques. De plus, ils peuvent facilement submerger les agents de votre centre d'assistance, en particulier s'ils doivent travailler avec des logs natifs, des outils basiques de gestion des verrouillages de comptes et des utilitaires d'analyse des événements. Le manque d'informations exploitables, la perte de données liée à l'encapsulage des logs et d'autres difficultés entraîneront inévitablement des longs retards, des coûts de support élevés et l'insatisfaction des utilisateurs qui ne peuvent pas travailler.

Change Auditor simplifie et accélère considérablement le dépannage des verrouillages. Il crée et stocke un événement complet et précis pour chaque verrouillage de compte, avec les cinq informations clés listées ci-dessus, dont le serveur ou la station de travail d'où provient le verrouillage de compte (voir Figure 2). Avec ces informations détaillées, votre centre d'assistance peut rapidement diagnostiquer et résoudre les verrouillages, gagnant ainsi un temps précieux tout en assurant la continuité de l'activité.

Si vous utilisez IT Security Search, qui est disponible avec plusieurs solutions Quest, dont Change Auditor, pour vos analyses forensiques, vous pouvez également rechercher facilement tous les événements d'un compte utilisateur ayant conduit à son verrouillage. Cela vous permet de comprendre la cause première des verrouillages persistants et peut vous indiquer qu'un problème plus grave pourrait se produire.

Conseil de professionnel : utilisez la fonctionnalité « restore value » (restaurer la valeur) dans Change Auditor pour déverrouiller immédiatement le compte lorsque votre analyse est terminée.

3. Modifications de l'appartenance à des groupes à privilèges

Les groupes à privilèges contrôlent l'accès aux ressources les plus importantes au sein de votre domaine. Les groupes à privilèges intégrés d'Active Directory, comme Administrateurs Entreprise et Administrateurs du domaine, sont extrêmement puissants. C'est pourquoi il est crucial de contrôler rigoureusement leurs appartenances. Toutefois, ce ne sont pas les seuls groupes que vous devez auditer. La plupart des entreprises créent également leurs propres groupes à privilèges. Souvent, ces groupes gèrent et sécurisent des données ou applications

En combien de temps votre équipe pourrait-elle dépanner des verrouillages si elle disposait de tous les détails clés dans un format standardisé et pertinent ?

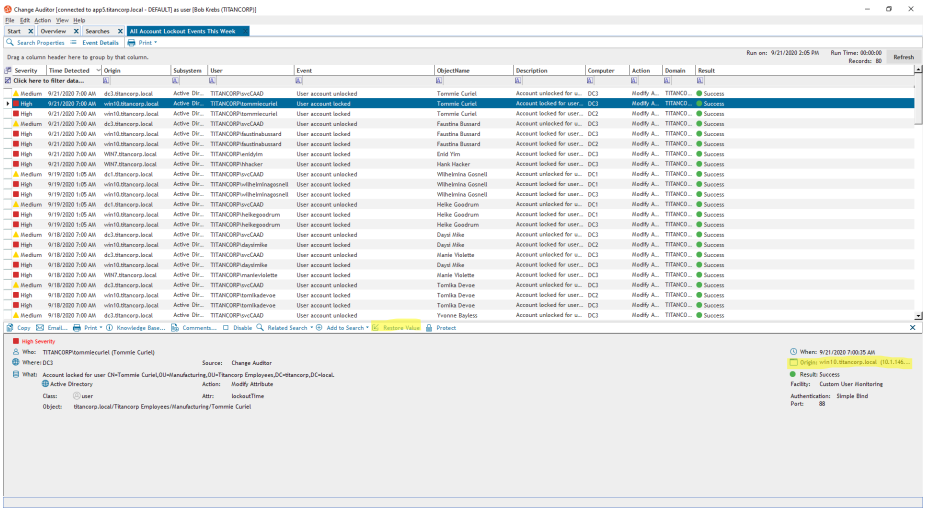


Figure 2. Change Auditor simplifie le dépannage des verrouillages en fournissant tous les détails clés, dont le serveur ou la station de travail d'où provient le verrouillage de compte.

Que se passerait-il si une personne mal intentionnée était ajoutée à votre groupe Administrateurs du domaine ? Change Auditor peut empêcher que cela ne se produise.

hautement sensibles. Ils doivent donc être surveillés de près.

Bien sûr, il n'est pas seulement vital de garder un œil sur tous vos groupes à privilèges pour maintenir la sécurité et la continuité de l'activité. Une étroite surveillance est également essentielle pour assurer la conformité et respecter de nombreuses réglementations, comme SOX, HIPAA ou RGPD. Les auditeurs internes et externes vous demanderont certainement comment vous auditez les modifications des appartenances à ces puissants groupes.

Change Auditor inclut une recherche prédéfinie qui vous permet de surveiller les groupes à privilèges intégrés en quelques clics. Vous pouvez facilement personnaliser cette recherche pour y ajouter les groupes à privilèges propres à votre entreprise et les groupes d'administration des serveurs locaux. Vous bénéficiez ainsi d'un plan complet pour auditer les modifications apportées à ces ressources importantes. De plus, Change Auditor envoie des alertes en temps réel sur les modifications apportées à l'appartenance des groupes, notamment l'ajout de nouveaux membres, une fonctionnalité indisponible nativement.

Cependant, pour vos groupes les plus sensibles, les rapports a posteriori et même les alertes en temps réel ne suffisent pas. Vous devez être en mesure d'empêcher proactivement les modifications des appartenances. Les outils natifs ne le permettent pas, mais Change Auditor propose une fonctionnalité de protection des objets qui vous permet de créer facilement une liste de vos groupes les plus critiques et d'interdire leur modification par qui que ce soit, même les utilisateurs qui appartiennent au groupe des administrateurs de domaine ou à un autre groupe à privilèges qui possède nativement les droits pour modifier l'appartenance aux groupes.

4. Activité des utilisateurs à privilèges

Selon une étude menée par Forrester, huit violations sur dix découlent directement d'une mauvaise utilisation ou d'un usage abusif de comptes d'administrateur ou d'accès à privilèges.

Les comptes à privilèges n'incluent pas uniquement tous vos administrateurs, ils comprennent aussi tous les comptes de service qui possèdent des droits élevés. La mauvaise utilisation de ces comptes peut entraîner de graves problèmes au sein de votre entreprise : temps d'arrêt, violations de données, échec des audits de conformité et atteinte durable à votre image de marque. Avec des outils natifs, il est extrêmement difficile de détecter à temps les actions inappropriées des utilisateurs à privilèges afin d'empêcher tous ces désagréments.

C'est pourquoi vous devez impérativement mettre en place une stratégie d'audit efficace pour les comptes à privilèges, et pas seulement pour identifier les modifications des appartenances, mais pour connaître l'activité de tout compte appartenant à un groupe à privilèges intégré ou propre à l'entreprise. Change Auditor vous permet d'auditer et de recevoir des alertes sur les modifications effectuées par les membres des groupes Administrateurs Entreprise et Administrateurs du domaine, et vous permet aussi de personnaliser facilement votre plan pour inclure vos propres comptes de service et même des utilisateurs spécifiques ayant accès à des données sensibles. Par exemple, imaginons qu'une application s'exécute sur le serveur X qui utilise le compte de service Y. Vous pouvez

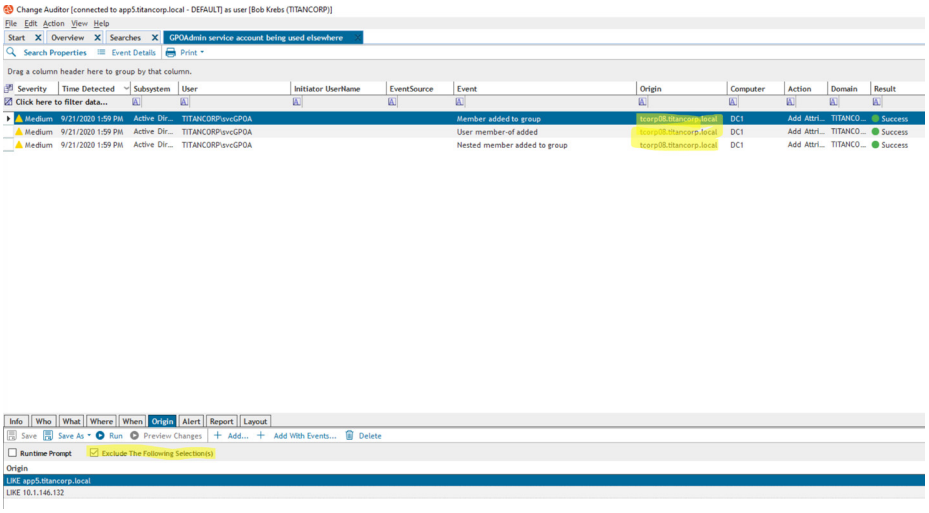


Figure 3. Identifiez rapidement toute activité inappropriée des utilisateurs à privilèges avec Change Auditor.

simplement définir une recherche et voir toutes les modifications effectuées par le compte de service Y qui ne proviennent pas du serveur X, montrant ainsi clairement une mauvaise utilisation des privilèges (voir Figure 3). Ce n'est là qu'un exemple de la flexibilité et de la puissance de Change Auditor parmi tant d'autres.

5. Création de nouveaux comptes d'utilisateur

La création d'un nouveau compte d'utilisateur dans Active Directory ouvre de nombreuses portes d'accès à votre environnement, dont Azure AD, si vous synchronisez AD avec le Cloud. Par conséquent, vous devez attentivement auditer ce type d'événement. Hélas, votre environnement est hautement dynamique et il est souvent difficile de distinguer un nouveau compte parfaitement légitime d'un compte clandestin malveillant.

Change Auditor peut vous aider. Pour commencer, si vous avez défini des alertes sur les modifications apportées à l'appartenance aux groupes à privilèges dont nous avons parlé précédemment, vous saurez immédiatement si un compte est créé et ajouté à n'importe lequel de ces groupes. Mais que diriez-vous d'adopter une approche un peu plus stratégique ? Si vous utilisez une structure de gestion des identités pour votre provisioning, comme votre système RH, il existe alors un compte qui effectue le provisioning. Ce compte doit donc être sécurisé dans votre système de gestion des accès à privilèges (PAM) ou autre. Toutes les tâches effectuées par ce compte qui ne respectent pas les paramètres définis par l'outil PAM sont considérées comme hautement suspectes. Vous pouvez très facilement définir une alerte en temps réel pour ce type d'activité dans Change Auditor : dans le champ de l'objet (WHAT), indiquez « user account creation » (création de compte d'utilisateur), remplissez le champ WHO (qui) avec le compte de service et utilisez « exclude the following » (exclure les éléments suivants) pour ignorer l'activité légitime du compte de service.

6. Modifications des contrôleurs de domaine

Vos contrôleurs de domaine (DC) sont à la tête de tout votre environnement Active Directory. Pour limiter les risques de connexions lentes, de faibles performances générales et même de pannes et défaillances catastrophiques, vous devez veiller à leur fonctionnement optimal. Autrement dit, il faut étroitement surveiller l'environnement pour identifier des modifications inappropriées effectuées par inadvertance et des attaques malveillantes.

Vous devez notamment vous défendre contre un type d'attaque en particulier qui vise à exfiltrer le fichier NTDS.dit de vos contrôleurs de domaine Active Directory, et qui utilise généralement un outil comme Volume Shadow Copy, PowerSploit ou NTDSUtil. Le fichier NTDS.dit stocke la plupart des données dans Active Directory (utilisateurs, groupes, ordinateurs, hachages de mots de passe utilisateur et configuration des annuaires). Aucune personne mal intentionnée ne doit donc mettre la main dessus.

Change Auditor fournit plusieurs rapports prêts à l'emploi qui montrent les modifications apportées au système de fichier, à la configuration, à l'état du système, au registre et aux services (comme toujours, en précisant les cinq éléments clés et les valeurs avant/après indispensables). Notre prochaine version vous permettra d'auditer les tentatives non autorisées d'accès au fichier NTDS.dit et même d'empêcher les attaquants de copier le fichier et de voler les données sensibles qu'il contient.

7. Authentifications et activité liée à la connexion

Le suivi automatisé, complet et fiable des authentifications et de l'activité de connexion/déconnexion des utilisateurs est essentiel en termes de sécurité et de conformité. Mais, à l'heure actuelle, la quantité de données et le niveau d'audit requis continuent de représenter un défi pour la plupart des entreprises. Avec le module Change Auditor Logon Activity, vous pouvez capturer toute cette activité et plus encore. Il collecte non seulement toute l'activité de connexion/déconnexion à AD, mais il consigne même l'intégralité des sessions du début à la fin, avec la raison de leur arrêt (déconnexion, mise hors tension, verrouillage d'écran). Si une ouverture de session échoue, vous pouvez connaître la raison de l'échec et obtenir les codes d'état pour dépanner le problème ou mener une analyse.

Change Auditor vous aide également à éliminer le protocole d'authentification NTLM, qui est bien moins sécurisé et plus facile à craquer que Kerberos. Change Auditor détecte et identifie clairement toutes les authentifications NTLM v1 et v2 pour que vous sachiez précisément quels utilisateurs et quelles applications continuent d'utiliser ces protocoles risqués (voir Figure 4).

Bien sûr, Kerberos présente aussi des failles. C'est pourquoi Change Auditor inclut également des rapports intégrés qui vous aident à détecter l'utilisation des vulnérabilités courantes observées lors d'attaques de type Golden Ticket et Pass-the-Ticket.

Comment pouvez-vous savoir si des comptes clandestins malveillants ont été créés sans crouler sous les alertes signalant des nouveaux comptes légitimes ? Grâce à Change Auditor.

Change Auditor vous aide à détecter les attaques de type Golden Ticket qui visent Kerberos et à éliminer le protocole d'authentification NTLM moins sécurisé.

Vous souhaitez recevoir des alertes et auditer tout votre environnement hybride depuis une console unique ? Il vous suffit d'associer One Demand Audit avec Change Auditor en quelques clics.

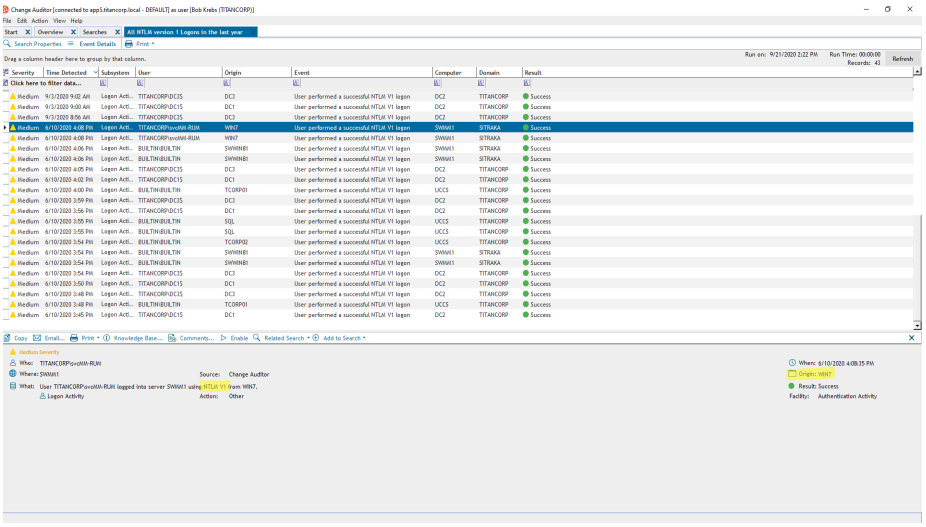


Figure 4. Un rapport Change Auditor intégré vous permet d'éliminer l'utilisation du protocole NTLM.

8. Connexions à Azure AD

Nous venons d'aborder l'activité d'ouverture de session pour Active Directory, mais qu'en est-il des connexions à Azure AD ? Si vous disposez d'un environnement hybride et utilisez des outils natifs, vous jonglez probablement entre plusieurs fenêtres et tentez difficilement de corréler des données d'événement disparates dans le but de comprendre comment les utilisateurs se connectent et ouvrent des sessions au sein de votre écosystème informatique.

Toutefois, en associant On Demand Audit avec Change Auditor, vous pouvez suivre l'activité locale et dans le Cloud depuis une seule interface. Toutes vos données Change Auditor locales sont transférées vers un tableau de bord hébergé dans le Cloud, qui est standardisé et corrélé pour que vous puissiez effectuer des recherches flexibles et visualiser les données de façon interactive. Mieux encore, le tableau de bord ne se limite pas aux données d'AD et Azure AD. Vous pouvez aussi auditer toutes les autres charges de travail Cloud, comme Exchange Online, SharePoint Online, OneDrive Entreprise et Teams. Toutes ces données hybrides peuvent être stockées de façon économique pendant 10 ans maximum. De plus, vous pouvez déléguer en toute sécurité les autorisations d'accès appropriées à vos équipes responsables de la sécurité et de la conformité (voir Figure 5).

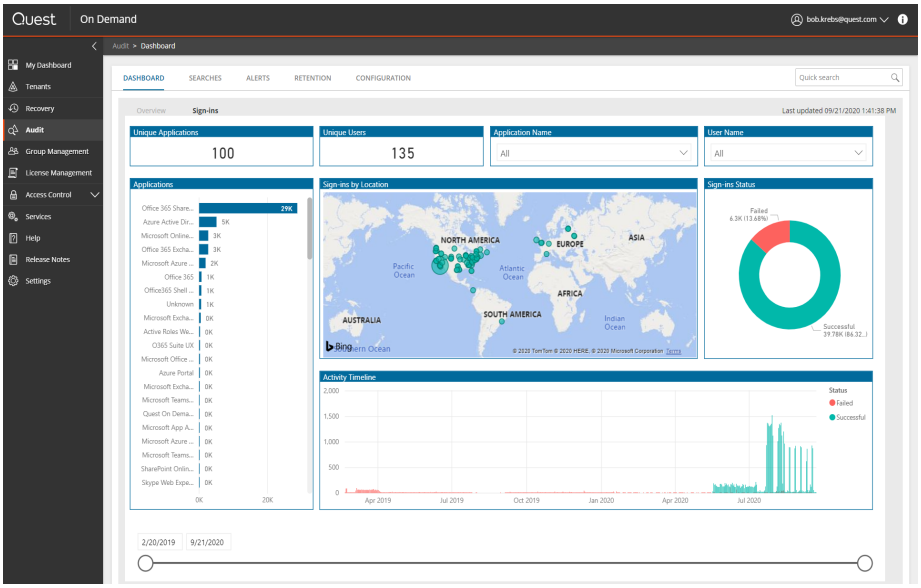


Figure 5. Suivez et visualisez l'activité au sein de votre environnement hybride depuis un tableau de bord unique.

9. Modifications des rôles Azure AD

Dans un environnement hybride, l'audit des groupes à privilèges locaux décrit précédemment n'est pas suffisant. Vous devez aussi surveiller toutes les modifications des rôles Azure AD, car ils permettent aux utilisateurs de gérer vos ressources Azure AD les plus stratégiques. Bien entendu, les pirates concentrent leurs efforts pour endosser ces rôles et ainsi accéder à vos données et applications les plus précieuses.

Une bonne pratique clé consiste à activer l'authentification multifacteur d'Azure AD pour tous les utilisateurs qui détiennent ces rôles, mais cela s'avère hélas insuffisant. Il faut également garder un œil sur les modifications des rôles Azure AD. Change Auditor vous facilite la tâche et vous permet de choisir si vous souhaitez recevoir des alertes proactives sur les modifications apportées aux rôles AD les plus critiques, comme Administrateur général, Administrateur d'authentification privilégié, Administrateur Exchange et Administrateur SharePoint.

Pour obtenir des informations plus détaillées sur les utilisateurs qui détiennent ces puissants rôles, la solution Enterprise Reporter de Quest est idéale. Elle offre une multitude de rapports intégrés que vous pouvez utiliser pour sécuriser efficacement ces rôles et présenter aux auditeurs internes ou externes qui souhaitent vérifier que vous avez mis en place des contrôles adéquats.

10. Audits internes

Si vous utilisez une solution d'audit pour protéger votre environnement Active Directory, vous devez vous assurer que l'outil lui-même n'est pas compromis ou mal utilisé. Par exemple, supposons qu'un individu malveillant parvienne à accéder au compte d'administration de l'outil : qu'est-ce qui l'empêchera d'apporter des modifications à votre écosystème informatique et à dissimuler les preuves en altérant ou en effaçant les enregistrements de votre solution d'audit ?

Change Auditor fournit une ligne de défense solide contre ce potentiel contournement de votre sécurité. Il comprend plus de 400 événements internes qui enregistrent les modifications apportées à sa configuration ou à son fonctionnement. Premièrement, l'outil capture toutes les connexions des clients à Change Auditor pour identifier précisément qui l'utilise. Il signale ensuite lorsque des agents sont stoppés, des modèles de protection sont supprimés et des événements spécifiques sont désactivés, ce qui vous permet de détecter toute activité suspecte susceptible de mettre en danger votre sécurité et votre conformité. L'outil surveille également si des tâches de purge sont ajoutées ou modifiées, ce qui indiquerait clairement que quelqu'un tente de couvrir ses agissements.

Conseil de professionnel : assurez-vous d'utiliser le champ « results » (résultats). Il est tout aussi important de connaître les tentatives infructueuses de modification que les modifications réussies qui ont eu lieu dans votre annuaire.

CONCLUSION

Avec l'augmentation de la complexité informatique et les menaces toujours plus nombreuses et sophistiquées, il est essentiel de contrôler attentivement votre environnement Active Directory local ou hybride. Vous ne pouvez tout simplement pas vous permettre de perdre des heures à décortiquer manuellement des logs d'événements obscurs ni à essayer de rassembler chaque élément d'information sur la situation. Vous avez besoin de disposer d'informations claires.

Change Auditor propose de nombreuses fonctionnalités puissantes pour vous aider à assurer la sécurité, la conformité, la productivité et la disponibilité. Il suit les modifications en temps réel, vous alerte en cas de modification critique et peut même empêcher la modification d'objets Active Directory essentiels. De plus, Change Auditor s'intègre en quelques clics avec On Demand Audit pour vous permettre de recevoir des alertes et d'auditer tout votre environnement hybride depuis une console unique. Vous pouvez même déléguer l'accès aux responsables, aux auditeurs et aux administrateurs de façon granulaire, afin de gagner un temps précieux sans pour autant compromettre la sécurité.

Pour en savoir plus, consultez la page https://www.quest.com/fr-fr/change-auditor/.

L'authentification multifacteur d'Azure AD limite l'utilisation de comptes d'administration Cloud, mais ne vous alerte pas quand un puissant rôle Azure AD est attribué à un individu. C'est possible avec Change Auditor.

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 les clients à relever leurs prochains défis informatiques dès à présent. Partout dans le monde, plus de 130 000 entreprises et 95 % de celles au classement Fortune 500 font confiance à Quest pour assurer une gestion et une surveillance proactives afin de soutenir toute nouvelle initiative des entreprises, de trouver toute solution à des défis Microsoft complexes et de garder une longueur d'avance sur les menaces à venir. Quest Software. Où demain rencontre aujourd'hui.

En cas de questions sur l'utilisation de ce document, nous vous invitons à contacter :
www.quest.com/fr-fr/company/contact-us.aspx