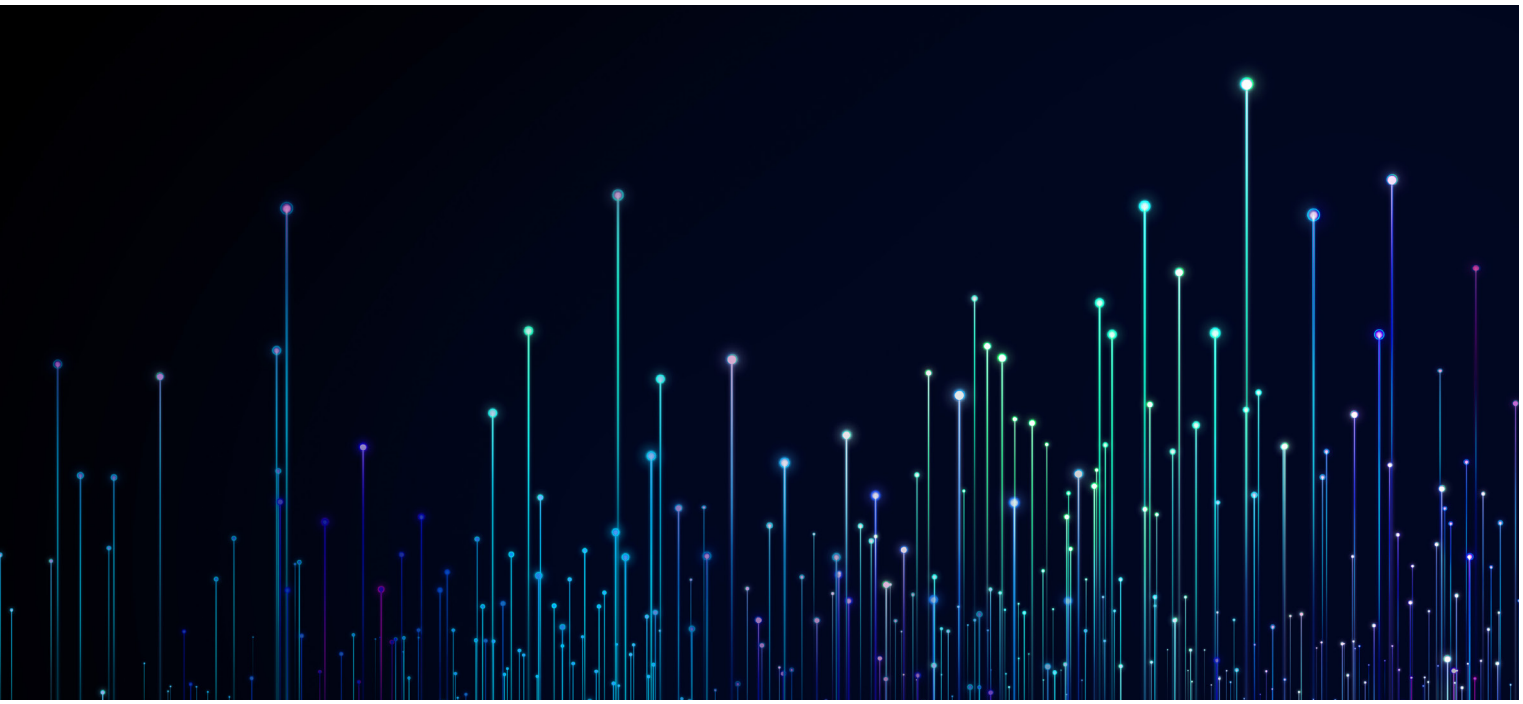
Die 10 wichtigsten Sicherheitsberichte und Warnmeldungen von Active Directory, die Sie benötigen

Stärken Sie Ihre Cybersicherheit und identifizieren Sie aktive Bedrohungen mit Change Auditor von Quest.



EINFÜHRUNG

Die klassische Verteidigung des Perimeters reicht einfach nicht mehr aus. Heute ist die Identität der neue Perimeter. Hacker nehmen aktiv Ihre Benutzerkonten ins Visier und nutzen kompromittierte Anmeldedaten mit dem Ziel, verheerenden Schaden in Ihrem Netzwerk anzurichten. De facto gibt es Berichten von Microsoft zufolge täglich Cyberangriffe auf 95 Mio. AD-Konten und 1,2 Mio. Azure AD-Konten werden pro Monat kompromittiert. Verschlimmernd hinzu kommen noch böswillige Insider und gestresste Mitarbeiter, die Leichtsinnsfehler machen. All das zeigt ganz klar, dass jede Organisation die Identifizierung von Bedrohungen in ihrer IT-Umgebung zu einer ihrer obersten Prioritäten machen muss.

Doch was bedeutet das konkret? Sicherheitsexperten empfehlen eine Strategie, bei der von Sicherheitsverletzungen ausgegangen wird. Sie sollen davon ausgehen, dass Sie bereits kompromittierte Konten und böswillige Insider in Ihrer IT-Umgebung haben und starke interne Sicherheitsprüfungen zum Schutz Ihrer wichtigsten und am häufigsten anvisierten Ressource implementieren: Active Directory. AD ist das Rückgrat Ihrer Organisation. Es kommt für die Authentifizierung und Autorisierung für jede kritische Ressource in Ihrer gesamten Umgebung zum Einsatz. Daher müssen Sie AD nicht bloß als Bestandteil der Infrastruktur, sondern als Sicherheitselement verwalten.

Change Auditor von Quest ist eine der leistungsfähigsten Lösungen, die Sie in Ihrem Sicherheitsarsenal haben können. In der schnelllebigen Welt von heute können Sie es sich schlicht nicht leisten, stundenlang Ereignisprotokolle zu durchkämmen und das durchaus reale Risiko einzugehen, kritische Ereignisse inmitten der ganzen Daten zu versäumen oder ein Ereignismuster zu übersehen, das auf einen Angriff hindeutet. Mit der Echtzeitüberwachung in Change Auditor wissen Sie direkt, was in Ihrer Umgebung passiert ist. So sparen Sie wertvolle Zeit und können gleichzeitig die Sicherheit stärken sowie die Einhaltung gesetzlicher Vorschriften gewährleisten. Sie haben mit Change Auditor sogar die Möglichkeit, Suchvorgänge zu starten und die Ergebnisse dann in nützliche und relevante Berichte und Warnmeldungen umzuwandeln – alles über eine zentrale Konsole.

In diesem Whitepaper werden die 10 wichtigsten Berichte und Warnmeldungen erläutert, die Sie zum Gewährleisten der Stabilität und Sicherheit Ihrer Active Directory Umgebung benötigen. Außerdem erfahren Sie, wie Sie diese Berichte und Warnmeldungen mit Change Auditor ganz einfach erhalten können.

Bereits eine einzige unzulässige Änderung an einem Gruppenrichtlinienobjekt kann zu einer Katastrophe führen. Mit Change Auditor können sie sofort über diese kritischen Ereignisse benachrichtigt werden.

DIE ZEHN WICHTIGSTEN CHANGE AUDITOR BERICHTE UND WARNMELDUNGEN

1. Änderungen an Gruppenrichtlinien

Gruppenrichtlinienobjekte gehören zu den wichtigsten Elementen Ihrer Infrastruktur. Bereits eine einzige unzulässige Änderung an einem Gruppenrichtlinienobjekt kann Ihre Sicherheit erheblich schwächen, weil Benutzer – oder Angreifer oder Malware, die sich gestohlene Anmeldedaten zunutze machen – dadurch beispielsweise imstande sind, Daten auf Flash-Laufwerke zu kopieren, die Eingabeaufforderung zu nutzen oder unerwünschte Anwendungen zu installieren.

Mit nativen Ereignisprotokollen wird zwar festgehalten, ob ein Gruppenrichtlinienobjekt aktualisiert wurde, aber nicht, welche Einstellungen konkret geändert wurden. Aus diesem Grund ist das Isolieren und Korrigieren von Problemen zeitaufwendig und fehleranfällig, weshalb Ihr Unternehmen auch über einen längeren Zeitraum gefährdet ist.

Da Change Auditor sich nicht nur auf native Protokolle stützt, kann die Lösung Ihnen umfassende Details zu Änderungen an Ihren Gruppenrichtlinienobjekten bereitstellen, einschließlich Einstellungen, Vererbung, Links und Status insgesamt. Zudem zeigt Change Auditor – anders als die nativen Überwachungstools – sämtliche Änderungsereignisse (inklusive Änderungen an Gruppenrichtlinienobjekten) in einem sinnvollen, vereinheitlichten Format sowie die fünf W und die überaus wichtigen Vorher-Nachher-Werte:

- Wer die Änderung vorgenommen hat
- Welches Objekt geändert wurde
- Wann das Objekt geändert wurde
- Was der Ausgangspunkt der Änderung war
- Welche Workstation für die Änderung verwendet wurde

Mit diesen kohärenten, detaillierten Informationen können Sie unerwünschte oder nicht genehmigte Änderungen an Ihren Gruppenrichtlinienobjekten schnell identifizieren und rückgängig machen, bevor Ihre Organisation dadurch zu Schaden kommt.

Change Auditor bietet aber nicht nur klare Berichte, sondern auch Echtzeitwarnmeldungen bei Änderungen Ihrer Wahl. Sie können sich insbesondere proaktiv über Änderungen an Ihren wichtigsten Gruppenrichtlinienobjekten benachrichtigen lassen – z. B. denen, die Ihre Kennwortrichtlinie und

Abbildung 1: Change Auditor liefert Angaben zu den fünf wesentlichen W jeder Änderung sowie die unerlässlichen Vorher-Nachher-Werte.

Kontosperrungsrichtlinie steuern – und so unmittelbar reagieren. Und noch besser: Change Auditor kann jeden davon abhalten, überhaupt erst Änderungen an wichtigen Active Directory-Objekten wie Gruppenrichtlinienobjekten vorzunehmen, ganz gleich, ob es sich um einen unachtsamen oder unerfahrenen Administrator oder einen Angreifer mit gestohlenen Anmeldedaten handelt.

Für umfassende Governance rund um Ihre Gruppenrichtlinienobjekte sollten Sie sich GPOADmin ansehen. Damit profitieren Sie von noch mehr Funktionen, beispielsweise für die rollenbasierte Zugriffssteuerung und Delegierung, den Versionsverlauf, Genehmigungs-Workflows, geplante Bereitstellungen und vollständige Rollbacks.

2. Benutzerkontensperrungen

Benutzerkontensperrungen sind nicht nur überaus frustrierend für die Benutzer, sie können auch wichtige Geschäftsprozesse zum Stillstand bringen. Außerdem können sie Ihre Helpdesk-Ressourcen überfordern, insbesondere, wenn diesen nur native Protokolle, elementare Tools für Kontosperrungen und Dienstprogramme zum Durchkämmen von Ereignissen zur Verfügung stehen. Der Mangel an nutzbaren Informationen, der Verlust von Daten wegen der Protokollverpackung und weitere Herausforderungen werden praktisch unausweichlich zu langen Verzögerungen, hohen Supportkosten und wütenden Benutzern führen, die ihre Aufgaben nicht erledigen können.

Change Auditor vereinfacht und beschleunigt den Prozess zur Fehlerbehebung bei Sperrungen deutlich. Die Lösung erstellt und speichert umfassende und präzise Ereignisse für jede Kontosperrung, inklusive Angaben zu den oben genannten fünf W, die auch Informationen zum Server oder der Workstation umfassen, von dem bzw. der die Kontosperrung ausgegangen ist (siehe Abbildung 2). Mit diesen detaillierten Informationen kann Ihr Helpdesk Sperrungen schnell diagnostizieren und beheben. So wird wertvolle Zeit gespart und ein unterbrechungsfreier Geschäftsbetrieb sichergestellt.

Falls Sie das als Teil verschiedener Lösungen von Quest (darunter auch Change Auditor) verfügbare Tool IT Security Search für Ihre forensischen Untersuchungen nutzen, können Sie ganz einfach Suchen für das Benutzerkonto ausführen und damit alle Ereignisse ausfindig machen, die zur Sperrung geführt haben. So können Sie die Ursache ständiger Sperrungen ermitteln und gegebenenfalls mysteriösere Dinge aufdecken, die vor sich gehen.

Hilfreicher Tipp: Verwenden Sie die Funktion zum Wiederherstellen von Werten in Change Auditor, um das Konto nach Ihrer Untersuchung unmittelbar zu entsperren.

3. Änderungen an Mitgliedschaften in privilegierten Gruppen

Privilegierte Gruppen steuern den Zugriff auf die wichtigsten Ressourcen in Ihrer Domäne. Die integrierten privilegierten Gruppen von Active Directory wie „Organisations-Admins“ und „Domänen-Admins“ verfügen über umfangreiche Rechte. Daher ist es nur vernünftig, die Mitgliedschaften in diesen Gruppen streng zu kontrollieren. Das sind aber noch längst nicht alle Gruppen, die Sie im Auge behalten sollten. Die meisten Organisationen erstellen auch eigene

Wie schnell könnte Ihr Team Fehlerbehebungen bei Sperrungen durchführen, wenn ihm alle wichtigen Details in einem sinnvollen, vereinheitlichten Format zur Verfügung stünden?

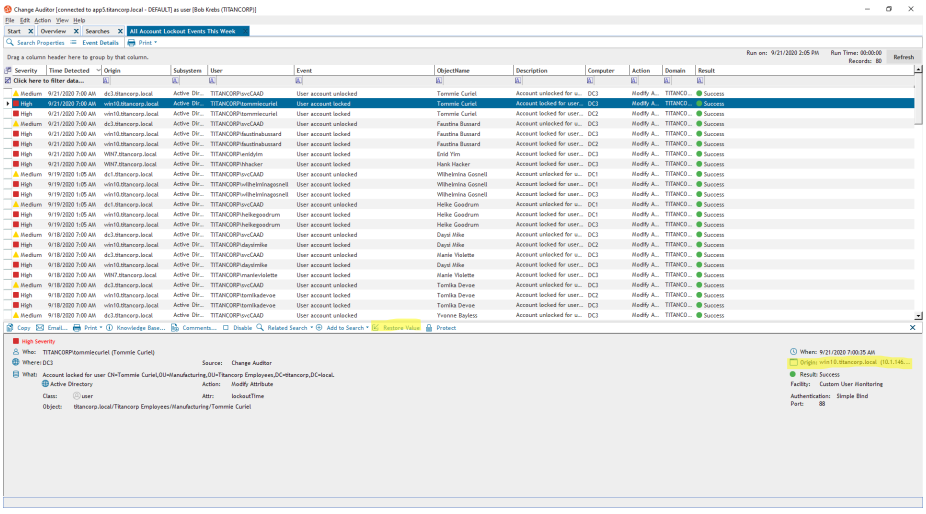


Abbildung 2: Change Auditor vereinfacht die Fehlerbehebung bei Sperrungen, indem alle wesentlichen Details bereitgestellt werden, einschließlich des Servers oder der Workstations, auf den bzw. die die Sperrung zurückzuführen ist.

Was wäre, wenn ein böswilliger Akteur zu Ihrer Domänen-Admins-Gruppe hinzugefügt würde? Mit Change Auditor können Sie verhindern, dass das jemals passiert.

privilegierte Gruppen. Diese Gruppen verwalten und sichern oft überaus sensible Daten oder Anwendungen und müssen deshalb sorgfältig überwacht werden.

Das genaue Beobachten Ihrer privilegierten Gruppen ist natürlich nicht nur für die Sicherheit und Business Continuity unerlässlich, sondern auch für die Compliance mit vielen behördlichen Vorschriften, vom SOX über den HIPAA bis hin zur DSGVO. Sowohl interne als auch externe Prüfer werden Sie mit Sicherheit fragen, wie Sie Änderungen an den Mitgliedschaften in diesen mächtigen Gruppen überwachen.

Change Auditor beinhaltet eine vordefinierte Suche, mit der Sie integrierte privilegierte Gruppen mit nur wenigen Klicks überwachen können. Sie können diese Suche problemlos anpassen, um Ihre unternehmensspezifischen privilegierten Gruppen und lokale Gruppen für die Serververwaltung aufzunehmen, sodass Sie über einen umfassenden Plan für die Überwachung von Änderungen an diesen wichtigen Ressourcen verfügen. Außerdem bietet Change Auditor Echtzeitbenachrichtigungen für Änderungen an Gruppenmitgliedschaften, beispielsweise auch für das Hinzufügen neuer Mitglieder – eine Funktion, die nativ nicht verfügbar ist.

Für Ihre sensibelsten Gruppen reichen Berichte nach dem Vorfall und sogar Echtzeitwarnmeldungen aber nicht aus. Sie müssen imstande sein, Mitgliedschaftsänderungen von vornherein proaktiv zu verhindern. Mit nativen Tools ist das nicht möglich, aber mit der Objektschutzfunktion von Change Auditor können Sie einfach eine Liste Ihrer wichtigsten Gruppen erstellen und Änderungen daran grundsätzlich verbieten, egal durch wen. Das gilt sogar für Benutzer, die den Domänen-Admins oder einer anderen privilegierten Gruppe angehören, die eigentlich über die Rechte zum Ändern von Gruppenmitgliedschaften verfügt.

4. Aktivitäten privilegierter Benutzer

Untersuchungen von Forrester zufolge sind acht von zehn Sicherheitsverletzungen die direkte Folge einer falschen oder missbräuchlichen Verwendung von Konten mit privilegiertem Zugriff und Administratorkonten.

Privilegierte Konten umfassen nicht nur alle Ihre Administratoren, sondern auch sämtliche Dienstkonten mit erweiterten Rechten. Der Fehlgebrauch dieser Konten kann ernste Probleme für Ihre Organisation nach sich ziehen: Ausfallzeiten, Datensicherheitsverletzungen, nicht bestandene Compliance-Prüfungen und eine anhaltende Schädigung Ihres Markenimage. Mit nativen Tools kann es sich jedoch als unglaublich schwierig erweisen, unangemessene Aktivitäten privilegierter Benutzer rechtzeitig zu identifizieren und so diese unangenehmen Folgen zu vermeiden.

Aus diesem Grund ist es unerlässlich, eine zuverlässige Überwachungsrichtlinie für privilegierte Konten zu implementieren – nicht nur für die gerade besprochenen Mitgliedschaften, sondern auch für die Aktivitäten eines jeden Kontos, das einer integrierten oder unternehmensspezifischen privilegierten Gruppe angehört. Mit Change Auditor können Sie nicht nur die Änderungen überwachen und melden lassen, die durch Mitglieder der Gruppe „Domänen-Admins“ oder „Organisation-Admins“ vorgenommen werden, sondern Ihren Plan auch mühelos anpassen, um Ihre individuellen Dienstkonten und sogar bestimmte

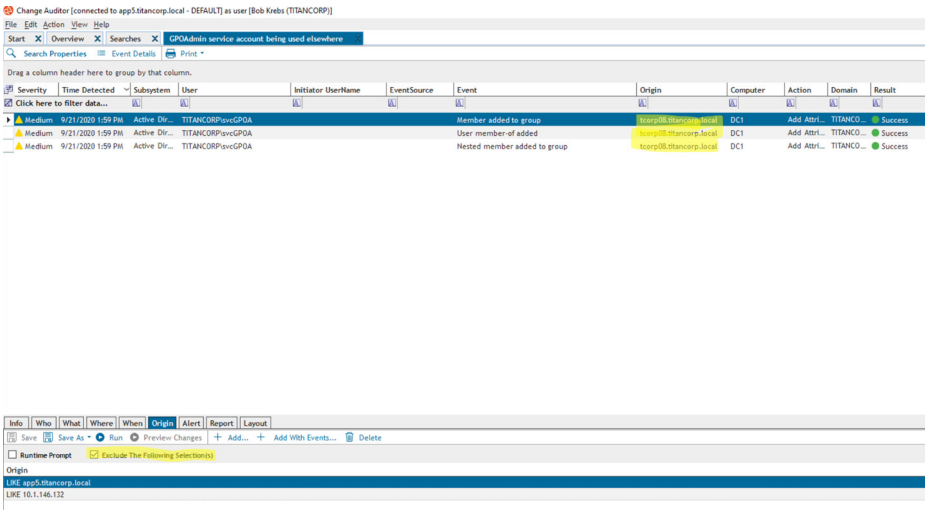


Abbildung 3: Mit Change Auditor können Sie unangemessene Aktivitäten privilegierter Benutzer schnell identifizieren.

Benutzer mit Zugriff auf sensible Daten aufzunehmen. Nehmen wir beispielsweise an, dass Sie über eine Anwendung verfügen, die auf Server X mit Dienstkonto Y ausgeführt wird. Sie haben die Möglichkeit, ganz einfach eine Suche einzurichten und sich ein Bild von sämtlichen Änderungen zu machen, die von Dienstkonto Y vorgenommen wurden und nicht auf Server X zurückzuführen sind. So können sie einen klaren Fehlgebrauch von Berechtigungen aufdecken (siehe Abbildung 3). Dies ist nur ein einfaches Beispiel für die Flexibilität und leistungsstarken Funktionen von Change Auditor.

5. Erstellung neuer Benutzerkonten

Die Erstellung neuer Benutzerkonten in Active Directory öffnet viele Türen zu Ihrer Umgebung, einschließlich Azure AD, wenn Sie Ihr AD in der Cloud synchronisieren. Diese Ereignisse müssen also sorgfältig geprüft werden. Doch da Ihre Umgebung ein äußerst dynamischer Ort ist, lässt sich womöglich nicht so leicht feststellen, ob es sich um ein durchaus angemessenes Konto oder ein nicht autorisiertes Backdoor-Konto handelt.

Hier kann Change Auditor Ihnen helfen. Wenn Sie wie soeben besprochen Benachrichtigungen für Änderungen an Mitgliedschaften in privilegierten Gruppen eingerichtet haben, werden Sie unmittelbar informiert, sobald ein Konto erstellt und einer Ihrer privilegierten Gruppen hinzugefügt wird. Doch wie wäre es mit einer etwas strategischeren Herangehensweise? Wenn die Provisionierung bei Ihnen über eine Art Identitäts-Framework wie z. B. Ihr HR-System stattfindet, gibt es ein Konto, das die Provisionierungsarbeit übernimmt, und dieses Konto sollte in Ihrem System zur Verwaltung des privilegierten Zugriffs (Privileged Access Management, PAM) oder auf andere Weise abgesichert werden. Alles, was das Konto außerhalb des PAM-Tools tut, ist äußerst suspekt. In Change Auditor können Sie ganz einfach Echtzeitbenachrichtigungen für solche Aktivitäten einrichten: Geben Sie im Feld WAS einfach „Erstellung von Benutzerkonten“ und im Feld WER das Dienstkonto an und verwenden Sie „Folgendes ausschließen“, um die legitimen Aktivitäten des Dienstkontos zu ignorieren.

6. Domänencontroller-Änderungen

Ihre Domänencontroller sind das Hirn Ihres gesamten Active Directory. Um das Risiko langsamer Anmeldevorgänge, einer schlechten Leistung insgesamt oder sogar katastrophaler Fehler und Ausfälle zu minimieren, müssen Sie sicherstellen, dass Ihre Domänencontroller einwandfrei funktionieren. Das bedeutet, dass Sie im Rahmen einer strengen Überwachung sowohl nach unangemessenen versehentlichen Änderungen als auch nach böswilligen Angriffen Ausschau halten müssen.

Ein besonders wichtiger Angriff, vor dem Sie sich schützen müssen, zielt auf die Exfiltrierung der Ntds.dit-Datei aus Ihren Active Directory-Domänencontrollern ab, in der Regel mithilfe eines Tools wie Volumeschattenkopie, PowerSploit oder NTDSUtil. Die NTDS.dit-Datei enthält den Großteil der Daten in Active Directory, einschließlich Benutzern, Gruppen, Computern, Benutzerkennwort-Hashes und Verzeichniskonfigurationen. Es ist also unbedingt zu vermeiden, dass diese Datei in die Hände eines böswilligen Akteurs gelangt.

Change Auditor bietet verschiedene vordefinierte Berichte zu den Änderungen, die das Dateisystem, die Konfiguration, den Systemstatus, die Registrierung und Services betreffen (wie immer mit Angaben zu den wichtigen fünf W und wesentlichen Vorher-Nachher-Werten). Halten Sie Ausschau nach unserem nächsten Release, mit dem Sie nicht autorisierte Zugriffsversuche auf die NTDS.dit-Datei überwachen und Angreifer sogar daran hindern können, die Datei zu kopieren und diese kritischen Daten zu stehlen.

> Wie können Sie über die Erstellung nicht autorisierter Backdoor-Konten informiert werden, ohne mit Benachrichtigungen zu legitimen neuen Konten überschüttet zu werden? Mit Change Auditor.

7. Authentifizierungen und Anmeldeaktivitäten

Das automatisierte, zuverlässige und umfassende Verfolgen von Benutzerauthentifizierungen und An-/Abmeldeaktivitäten ist für die Sicherheit und Compliance unerlässlich. Die Menge an Daten und das Ausmaß der erforderlichen Überwachung stellt jedoch für die meisten Organisationen aktuell nach wie vor eine Herausforderung dar. Mit dem Modul für Anmeldeaktivitäten von Change Auditor können Sie alle diese Aktivitäten und mehr erfassen. Es werden nicht nur sämtliche AD-An- und Abmeldeaktivitäten zusammengetragen, sondern auch ganze Benutzersitzungen von Anfang bis Ende ermittelt, inklusive der Gründe für die Beendigung (Abmeldung, Abschaltung, Sperrbildschirm). Wenn ein Anmeldefehler auftritt, erhalten Sie Informationen zu den Gründen für den Anmeldefehler sowie Statuscodes, die für die Fehlerbehebung oder forensische Untersuchung hilfreich sein können.

Change Auditor hilft Ihnen auch, das NTLM-Authentifizierungsprotokoll, das deutlich weniger sicher und einfacher zu knacken ist als Kerberos, aus Ihrer Umgebung zu verbannen. Change Auditor erkennt und identifiziert eindeutig alle Authentifizierungen mit NTLM v1 und v2,

> Change Auditor hilft Ihnen, Kerberos Golden Ticket-Angriffe zu identifizieren und das weniger sichere NTLM-Authentifizierungs-protokoll zu verbannen.

Sie möchten eine einzige Konsole für die Überwachung und Warnmeldungen für Ihre gesamte Hybridumgebung nutzen? Kombinieren Sie einfach On Demand Audit und Change Auditor – mit nur wenigen Klicks.

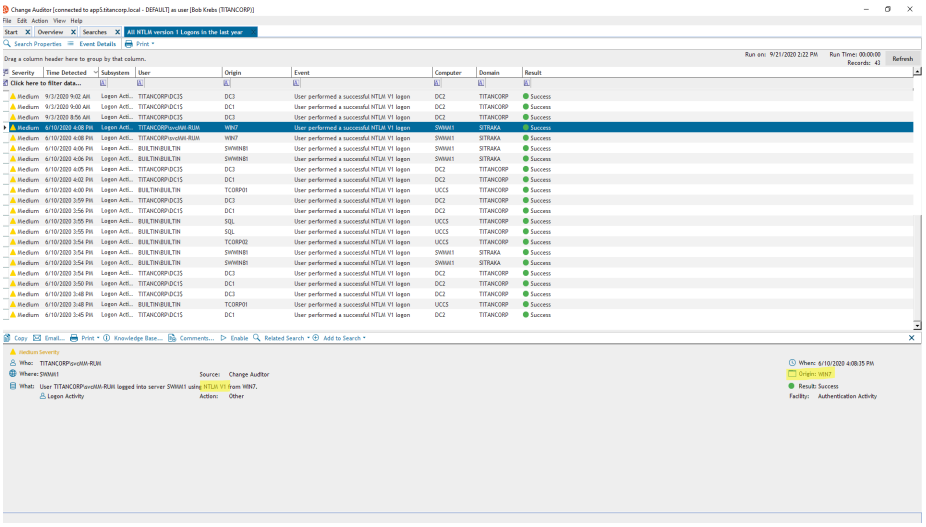


Abbildung 4: Ein integrierter Change Auditor-Bericht hilft Ihnen, das NTLM-Protokoll aus Ihrer Umgebung zu verbannen.

sodass Sie genau sehen können, welche Benutzer und Anwendungen nach wie vor diese riskanten Protokolle nutzen (siehe Abbildung 4).

Natürlich hat auch Kerberos Schwachstellen. Aus diesem Grund umfasst Change Auditor auch integrierte Berichte, die Ihnen helfen, die Ausnutzung gängiger Sicherheitslücken bei Golden Ticket- und Pass-the-Ticket-Angriffen zu identifizieren.

8. Azure AD-Anmeldungen

Wir haben gerade über Anmeldeaktivitäten für Active Directory gesprochen, doch wie sieht es mit Azure AD-Anmeldungen aus? Wenn Sie über eine hybride Umgebung verfügen und mit nativen Tools arbeiten, haben Sie mit mehreren Bildschirmen zu kämpfen und müssen sich abquälen, um separate Ereignisdaten zu korrelieren und sich so ein Bild von sämtlichen Anmeldeaktivitäten in Ihrer IT-Umgebung machen zu können.

Durch die Kombination von On Demand Audit mit Change Auditor können Sie jedoch sämtliche Aktivitäten vor Ort und in der Cloud über eine einzige Oberfläche nachverfolgen. Alle Ihre lokalen Change Auditor Daten werden in ein gehostetes Dashboard in der Cloud übertragen, vereinheitlicht und korreliert und stehen dann für flexible Suchen und interaktive Datenvisualisierungen zur Verfügung. Das Dashboard ist sogar nicht nur auf AD- und Azure AD-Auditdaten beschränkt, sondern ermöglicht auch die Prüfung aller

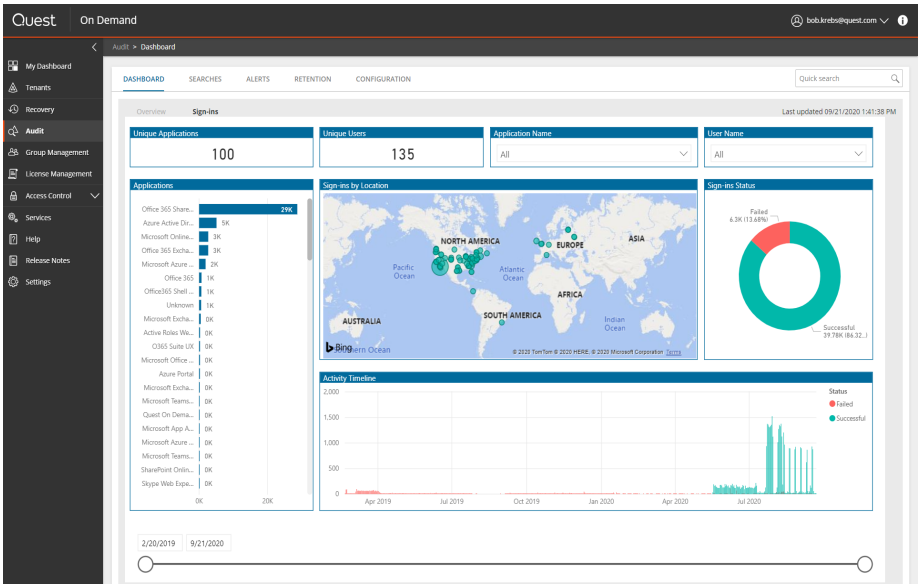


Abbildung 5: Verfolgen und visualisieren Sie Aktivitäten in Ihrer gesamten Hybridumgebung mit nur einem Dashboard.

anderen Cloud-Workloads wie Exchange Online, SharePoint Online, OneDrive for Business und Teams! Alle diese hybriden Daten können auf kosteneffiziente Weise für bis zu 10 Jahre gespeichert werden und Sie können angemessene Zugriffsberechtigungen sicher an Ihre Sicherheits- und Compliance-Teams delegieren (siehe Abbildung 5).

9. Azure AD-Rollenänderungen

In einer hybriden Welt reicht es nicht aus, Ihre lokalen privilegierten Gruppen wie zuvor beschrieben zu kontrollieren. Sie müssen auch sämtliche Änderungen an Azure AD-Rollen überwachen, da sie Benutzern die Verwaltung Ihrer wichtigsten Azure AD-Ressourcen ermöglichen. Hacker zielen natürlich darauf ab, in diese Rollen zu schlüpfen, um auf Ihre wertvollen Daten und Anwendungen zugreifen zu können.

Das Aktivieren der Multi-Faktor-Authentifizierung (MFA) von Azure AD für alle Benutzer, denen diese Rollen zugewiesen sind, ist eine wichtige Best Practice – aber leider nicht ausreichend. Sie müssen auch Änderungen an Azure AD-Rollen genau im Auge behalten. Mit Change Auditor ist das eine einfache Aufgabe und Sie können auch proaktive Warnmeldungen bei Änderungen an Ihren wichtigsten AD-Rollen wie „Globaler Administrator", „Privilegierter Authentifizierungsadministrator", „Exchange Administrator" und „SharePoint Administrator" aktivieren.

Eine noch gründlichere Prüfung der Mitglieder mit diesen mächtigen Rollen ermöglicht Enterprise Reporter von Quest. Die Lösung bietet verschiedene integrierte Berichte, mithilfe derer Sie diese Rollen unter Verschluss halten können. Zudem können Sie die Berichte internen oder externen Prüfern zur Verfügung stellen, um zu belegen, dass Sie angemessene Kontrollen implementiert haben.

10. Interne Überwachung

Wenn Sie zum Schützen Ihres Active Directory auf eine Überwachungslösung setzen, müssen Sie sichergehen können, dass das Tool selbst nicht kompromittiert wurde oder missbräuchlich verwendet wird. Nehmen wir beispielsweise an, dass ein böswilliger Akteur Zugriff auf das Administratorkonto des Tools erhält. Was hindert ihn dann daran, nach Belieben Änderungen in Ihrer IT-Umgebung vorzunehmen und die Beweise anschließend zu beseitigen, indem er die Datensätze in Ihrer Überwachungslösung ändert oder löscht?

Change Auditor bietet robuste Maßnahmen zur Vermeidung einer solchen Umgehung Ihrer Sicherheitsvorkehrungen. Die Lösung umfasst 400 interne Ereignisse zur Erfassung von Änderungen, die die Konfiguration oder Funktionsweise der Lösung betreffen. Zunächst werden alle Client-Anmeldungen bei Change Auditor erfasst, sodass Sie genau wissen, wer die Lösung verwendet hat. Es werden aber auch Berichte über gestoppte Agenten, entfernte Schutzvorlagen und die Deaktivierung bestimmter Ereignisse erstellt, sodass Sie verdächtige Aktivitäten identifizieren können, die die Sicherheit und Compliance beeinträchtigen könnten. Die Lösung verfolgt auch hinzugefügte oder geänderte Bereinigungsaufträge, die definitiv darauf hinweisen könnten, dass jemand seine Spuren verwischen will.

Hilfreicher Tipp: Nutzen Sie das Ergebnisfeld. Es ist genauso wichtig, über fehlgeschlagene Änderungsversuche Bescheid zu wissen wie über erfolgreiche Änderungen in Ihrem Verzeichnis.

FAZIT

In Anbetracht der steigenden IT-Komplexität und immer zahlreicheren und ausgeklügelteren Bedrohungen ist es unerlässlich, mit Blick auf Ihre lokale oder hybride Active Directory-Umgebung die Oberhand zu behalten. Sie können es sich schlicht nicht leisten, Stunden mit dem manuellen Durchkämmen kryptischer Ereignisprotokolle zu verbringen und zu versuchen, sämtliche Puzzlestücke zu einem Gesamtüberblick zusammenzufügen. Sie brauchen klare Informationen, die direkt bereitstehen.

Change Auditor bietet zahlreiche leistungsstarke Funktionen, mit denen Sie Sicherheit, Compliance, Produktivität und Verfügbarkeit gewährleisten können. Die Lösung verfolgt Änderungen in Echtzeit, benachrichtigt Sie über wichtige Änderungen und kann sogar verhindern, dass Änderungen an kritischen Active Directory-Objekten vorgenommen werden. Zudem ermöglicht Change Auditor die Integration mit On Demand Audit in nur wenigen Klicks, sodass Sie eine einzige Konsole für die Überwachung Ihrer gesamten Hybridumgebung und das Prüfen entsprechender Benachrichtigungen nutzen können. Sie haben sogar die Möglichkeit zum granularen Delegieren des Zugriffs an Manager, Prüfer und Administratoren, sodass Sie wertvolle Zeit sparen, ohne dass die Sicherheit beeinträchtigt wird.

Weitere Informationen finden Sie unter https://www.quest.com/de-de/change-auditor/.

Die MFA von Azure AD beschränkt die Nutzung von Cloud-Admin-Konten, benachrichtigt Sie aber nicht, wenn jemandem eine starke Azure AD-Rolle zugewiesen wird. Change Auditor schon.

ÜBER QUEST

Quest stellt Softwarelösungen bereit, die die Vorteile neuer Technologien in einer immer komplexeren IT- Landschaft real werden lassen. Von der Datenbank- und Systemverwaltung über die Verwaltung von Active Directory und Office 365 bis zur Cyber-Resilienz: Quest hilft Kunden, bereits jetzt ihre nächste IT-Herausforderung zu bewältigen. Weltweit vertrauen mehr als 130.000 Unternehmen und 95 % der Fortune 500 Quest die proaktive Verwaltung und Überwachung für die nächste Unternehmensinitiative sowie die Bestimmung der nächsten Lösung für komplexe Microsoft Herausforderungen an, um für die nächste Bedrohung gewappnet zu sein. Quest Software - Der Zukunft einen Schritt voraus.

Sollten Sie Fragen hinsichtlich der potenziellen Nutzung des Materials haben, wenden Sie sich bitte an:
www.quest.com/de-de/company/contact-us.aspx