Change Auditor

Audyt zmian w czasie rzeczywistym
dla środowiska platformy Microsoft

Rejestrowanie zdarzeń i raportowanie zmian dla aplikacji i usług w przedsiębiorstwie jest uciążliwe, czasochłonne i w niektórych przypadkach niemożliwe przy użyciu natywnych narzędzi audytorskich. Ponieważ nie ma centralnej konsoli, należy powtarzać proces dla każdego serwera, a w rezultacie otrzymujemy ogromną ilość danych bez kontekstu przy dużej ilości raportów.

Oznacza to, że udowodnienie zgodności lub szybkie reagowanie na zdarzenia jest ciągłym wyzwaniem. Podobnie, bezpieczeństwo danych jest zagrożone, ponieważ przy natywnym audycie zdarzeń szczegółowe dane są rzadkie i trudne do zinterpretowania. W związku z tym o problemach można się dowiedzieć dopiero wtedy, gdy jest już za późno. A ponieważ natywne narzędzia nie mogą uniemożliwić uprzywilejowanemu użytkownikowi wyczyszczenia dziennika zdarzeń, można stracić dane z dziennika - przez co audyt w ogóle straci cel.

Na szczęście jest Quest® Change Auditor. Ta rodzina produktów umożliwia audytowanie, ostrzeganie i raportowanie wszystkich zmian wprowadzonych do Active Directory (AD), Azure AD, Exchange, Office 365, SharePoint, Skype for Business, VMware, EMC, NetApp, SQL Server i serwerów plików Windows, a także zapytań LDAP w stosunku do AD - wszystko to w czasie rzeczywistym i bez konieczności przeprowadzania audytu natywnego.

Można je łatwo zainstalować, wdrożyć i zarządzać swoim środowiskiem z jednej centralnej konsoli. Każde zdarzenie i wszystkie inne związane z nim akcje są wyświetlane w prosty sposób, dając informację kto, co, kiedy, gdzie i skąd dokonał zmian oraz informację o poprzednich i aktualnych ustawieniach.

KORZYŚCI:

- Wyeliminuj nieznane problemy związane z bezpieczeństwem, zapewnij stały dostęp do aplikacji, systemów i użytkowników poprzez śledzenie wszystkich zdarzeń i zmian;
- Zmniejsz napięcia i złożoności poprzez automatyczną interpretację kryptograficznych danych w celu szybszego reagowania i lepszego podejmowania decyzji;
- Zmniejsz ryzyko zagrożenia bezpieczeństwa w ciągu kilku sekund dzięki alarmom wysyłanym w czasie rzeczywistym do dowolnego urządzenia w celu natychmiastowej reakcji, w biurze lub poza nim;
- Zmniejsz spadki wydajności na serwerach poprzez zbieranie zdarzeń bez korzystania z audytu natywnego;
- Usprawnij sprawozdawczość w zakresie zgodności, dedykowaną dla polityk wewnętrznych oraz regulacji zewnętrznych, w tym w systemach SOX, PCI DSS, HIPAA, FISMA, SAS 70 i innych.
- Zapewnij kierownictwu i audytorom dowody odpowiednich kontroli informatycznych.

Dzięki narzędziu Change Auditor uzyskasz informacje o tym, kto, co, kiedy, gdzie i z jakiej stacji roboczej dokonał zmian, w porządku chronologicznym.

Tak szeroki zakres analizy danych umożliwia podjęcie natychmiastowych działań w przypadku pojawienia się kwestii, takich jak to, jakie zmiany zostały wprowadzone przez konkretnych użytkowników i z których stacji roboczych, bez konieczności domyślania się pochodzenia problemów związanych z bezpieczeństwem. Niezależnie, czy staramy się sprostać rosnącym wymaganiom w zakresie zgodności z przepisami, czy mamy na celu rozwijanie wewnętrznych zasad bezpieczeństwa, Change Auditor jest rozwiązaniem, na którym można polegać.

FUNKCJE:

- **Audyt środowiska hybrydowego z widokiem skorelowanym** - audyt środowiska hybrydowego, w tym AD/Azure AD, Exchange/Exchange Online, SharePoint/SharePoint Online/OneDrive for Business, a także logowania AD i Azure AD sign-ins. W odróżnieniu od audytu natywnego, Change Auditor oferuje pojedynczy, skorelowany widok aktywności w środowiskach hybrydowych, zapewniając widoczność wszystkich dokonujących się zmian - czy to w lokalu firmy, czy w chmurze;
- **Zapobieganie zmianom -** ochrona przed zmianami krytycznych danych w serwerach plików AD, Exchange i Windows, w tym grup uprzywilejowanych, obiektów Group Policy i wrażliwych skrzynek mailowych;
- **Gotowy raport dla audytora -** tworzenie kompleksowych sprawozdań dotyczących najlepszych praktyk i mandatów w zakresie zgodności z przepisami dla systemów SOX, PCI DSS, HIPAA, FISMA, GLBA, PKBR i innych;
- **Hosted dashboard z usługą On Demand Audit** - wyświetlanie hybrydowej aktywności AD i Office 365 razem z hostowanym dashboardem SaaS z szybkim wyszukiwaniem, interaktywną wizualizacją danych i długoterminowym przechowywaniem zdarzeń;
- **Wykrywanie Golden Tickets -** wykrywanie i alarmowanie o typowych lukach w autoryzacji Kerberosa, wykorzystywanych podczas wystawiania Złotych Biletów (golden tickets - ataki typu pass-the-ticket);
- **Wysokowydajny silnik audytowy** - stosuje ograniczenia audytowe i przechwytuje informacje o zmianach bez konieczności tworzenia natywnych dzienników audytów, co skutkuje szybszymi wynikami i znacznymi oszczędnościami zasobów pamięci masowej;
- **Blokada konta -** przechwytywanie adresu IP i nazwy stacji roboczej dla zdarzeń blokady konta oraz przeglądanie związanych z tym logowaniem i próbami dostępu w interaktywnej osi czasu. Pomaga to uprościć wykrywanie i badanie wewnętrznych i zewnętrznych zagrożeń dla bezpieczeństwa;

„Nasi pentesterzy byli zaskoczeni, że nie mogli obejść zabezpieczenia obiektu w Change Auditorze."

Administrator w dużej sieci handlowej

- **Alerty w czasie rzeczywistym w ruchu -** wysyła alerty o krytycznych zmianach poprzez wiadomości e-mail i do urządzeń przenośnych, aby natychmiast podjąć działania, co pozwoli na szybszą reakcję na zagrożenia, nawet będąc poza lokalizacją;
- **Zintegrowane przekierowywanie zdarzeń** – łatwa integracja z rozwiązaniami SIEM w celu przekierowania zdarzeń audytora do Splunk, ArcSight lub QRadar. Dodatkowo, ChangeAuditor integruje się z Quest® InTrust® w celu skompresowanego przechowywania zdarzeń w formacie 20:1 i scentralizowanego zbierania i analizy dzienników oraz alarmowania i podejmowania automatycznych działań w odpowiedzi na podejrzane zdarzenia.

„Wcześniej dojście do problemu mogło zająć nawet godzinę. Change Auditor skrócił ten czas do 5-10 minut.

Dennis Persson, Technik IT, Region Hallnd

O Quest

Quest dostarcza rozwiązania programowe dla szybko zmieniającego się świata informatyki korporacyjnej. Pomagamy uprościć wyzwania związane z wielką ilością danych, ekspansją chmury obliczeniowej, hybrydowymi centrami danych, zagrożeniami dla bezpieczeństwa oraz wymogami prawnymi.

Nasze portfolio obejmuje rozwiązania do:

- zarządzania bazami danych;
- ochrony danych;
- ujednoliconego zarządzania punktami końcowymi;
- zarządzania tożsamością i dostępem;
- zarządzania platformą Microsoft.

Masz pytania? Skontaktuj się z nami:

Greeneris Sp. z o.o. jesteśmy oficjalnymi przedstawicielami firmy Quest.
Jeśli chcesz dowiedzieć się więcej o rozwiązaniach Quest zadzwoń do nas:
+48 22 439 03 20 lub wyślij email: biuro@greeneris.com.
www.greeneris.com