Quest Security Guardian

Uprzedzaj cyberataki na Active Directory dzięki Security Guardian, który wskaże co się wydarzyło, co zostało ujawnione i jak rozwiązać problem.

Quest Security Guardian to rozwiązanie dla bezpieczeństwa Active Directory zaprojektowane w celu zmniejszenia ryzyka ataków. Z uproszczonego, ujednoliconego obszaru roboczego, Security Guardian redukuje liczbę alertów poprzez priorytetyzację najbardziej podatnych na ataki luk i konfiguracji Active Directory. Security Guardian pokazuje, co się stało, czy jesteś narażony i jak naprawić problem.

Chroń swoje krytyczne zasoby dzięki:

- Porównanie bieżącej konfiguracji Active Directory z najlepszymi praktykami.
- Blokowanie krytycznych obiektów, w tym GPO, przed błędną konfiguracją i naruszeniem bezpieczeństwa.
- Wyprzedzaj zagrożenia, stale monitorując wskaźniki narażenia (IOE) i wskaźniki kompromisu (IOC).

Zabezpieczenie tożsamości jest niezbędne do utrzymania ciągłości biznesowej w całej organizacji - zwłaszcza Active Directory (AD). Konsekwencje przestoju AD mogą być dramatyczne, a koszty sięgają nawet 730 tysięcy dolarów na godzinę, jak donosi Forrester Consulting.

Ponadto, biorąc pod uwagę, że 80 procent naruszeń wiąże się obecnie z wykorzystaniem zagrożonych tożsamości, AD stało się głównym celem. Quest Security Guardian pomoże zredukować ryzyko ataku na AD w prosty i szybki sposób.

Ocena bezpieczeństwa AD

Analiza porównawcza bieżącej konfiguracji Active Directory z wcześniej zdefiniowanymi najlepszymi praktykami. Będziesz mieć pełny wgląd w IOE, IOC i zasoby warstwy zerowej. To narzędzie bezpieczeństwa Active Directory nie tylko pomaga w ograniczaniu zagrożeń, ale także w zmniejszaniu ryzyka ataku.

Koncentracja na zasobach krytycznych

Identyfikuj i ustalaj priorytety zasobów warstwy zerowej, zapewniając skupienie największej uwagi na najbardziej podatne na ataki komponenty. Uzyskaj pełną kontrolę nad zasobami krytycznymi, umożliwiając dynamiczne modyfikowanie listy warstwy zerowej, dzięki czemu zawsze jesteś dostosowany do zmieniających się potrzeb organizacji.

Korzyści:

- Zmniejsz ryzyko ataku, przygotowując swoją Active Directory pod kątem najlepszych praktyk.
- Uprość zabezpieczenia AD dzięki pełnej widoczności, kontroli i ochronie krytycznych zasobów.
- Uprość konfigurację AD i bądź o krok przed atakującymi.
- Unikaj nadmiernej ilości alertów i identyfikuj rzeczywiste zagrożenia, koncentrując się na alertach o wysokiej wartości.
- Uzyskaj współdziałanie sygnałów bezpieczeństwa IOC i IOE, zapewniających szybką reakcję na zagrożenia.

greeneris

Greeneris Sp. z o.o. | Adres: ul. Wojciecha Korfantego 5, 01-496 Warszawa, Polska
Tel. +48 22 439 03 20 | biuro@greeneris.com | www.greeneris.com

Zapobieganie zagrożeniom AD

Zabezpiecz krytyczne obiekty AD przed kompromitacją i błędną konfiguracją, w tym wrażliwe obiekty GPO. Security Guardian dostarcza szczegółowe raporty o stanie obiektów, zapewniając dane potrzebne do podjęcia odpowiednich działań.

Wykrywanie zagrożeń w usłudze AD

Korzystając z Security Guardian będziesz na bieżąco ograniczał zagrożenia, oraz będziesz dobrze przygotowany do szybkiej reakcji na potencjalne incydenty bezpieczeństwa.

Szybka reakcja na incydenty

Dowiedz się kto, co, gdzie, jak i kiedy wykonywał podejrzane działania dzięki inteligentnym i kontekstowym powiadomieniom, które pomogą zmniejszyć nadmiar alertów. Możliwe jest bezproblemowe przekazywanie IOE i IOC do narzędzi SIEM, takich jak np. Microsoft Sentinel i Splunk, w celu płynnej integracji i scentralizowanej widoczności.

Uproszczony, ujednolicony widok zabezpieczeń AD

Skoncentruj się na podstawowych operacjach dzięki przyjaznemu interfejsowi użytkownika, który zapewnia wgląd w IOE, IOC i inne parametry bezpieczeństwa.

QUEST:

Quest Software jest producentem oprogramowania, które wspiera korzyści płynące z nowych technologii w coraz bardziej złożonym środowisku IT. Od zarządzania bazami danych i systemami, po zarządzanie Active Directory i Office 365 oraz odporność na cyberzagrożenia.

Quest Software. Where next meets now.

Dowiedz się więcej o rozwiązaniach Quest Software

kontakt.greeneris.com/quest

Masz pytania? Skontaktuj się z nami

Nasi specjaliści pomogą Państwu w sprecyzowaniu wymagań. Ocenimy bieżące systemy oraz środowisko IT pod kątem potencjalnych zagrożeń oraz pomożemy w doborze najkorzystniejszych rozwiązań prewencyjnych.
Zadzwoń do nas **+48 22 439 03 20** lub napisz **biuro@greeneris.com**

www.greeneris.com

greeneris