Quest Security Guardian

Seien Sie Cyberangriffen auf Active Directory immer einen Schritt voraus – mit einer AD-Sicherheitslösung, die aufzeigt, was passiert ist, welche Systeme und Daten gefährdet sind und wie Sie das Problem beheben können.

Quest Security Guardian ist ein Active Directory-Sicherheits-Tool, das Ihre Angriffsfläche verkleinert. Mit einer vereinfachten, einheitlichen Arbeitsumgebung reduziert Security Guardian die Müdigkeit, die mit zu vielen Warnmeldungen einhergeht, indem es die anfälligsten Schwachstellen und Active Directory-Konfigurationen, die Aufmerksamkeit erfordern, priorisiert. Die Lösung zeigt auf, was passiert ist, ob Sie gefährdet sind und wie Sie das Problem beheben können.

Schützen Sie Ihre kritischen Tier-0-Assets mit folgenden Möglichkeiten:

- Benchmarking der aktuellen Active Directory-Konfiguration im Vergleich mit Best Practices aus der Branche
- Schutz kritischer Objekte, einschließlich GPOs, vor Fehlkonfigurationen und Kompromittierung
- Kontinuierliche Überwachung auf Indikatoren für eine Gefährdung (Indicators of Exposure, IOEs) und Indikatoren für eine Kompromittierung (Indicators of Compromise, IOCs), damit Sie Bedrohungen immer einen Schritt voraus sind

Identitätssicherheit ist für die Aufrechterhaltung der Business Continuity in Ihrem Untrnehmen unerlässlich – insbesondere bei Active Directory (AD). Die Folgen von AD-Ausfallzeiten sind verheerend. Die Kosten belaufen sich auf bis zu 730.000 US-Dollar pro Stunde, wie Forrester Consulting berichtet. Angesichts der Tatsache, dass inzwischen 80 % der Sicherheitsverletzungen auf kompromittierte Identitäten zurückzuführen sind, ist AD natürlich ein bevorzugtes Ziel. Mit Quest Security Guardian können Sie Ihre AD-Angriffsfläche schnell und unkompliziert verkleinern.

AD-Sicherheitsbewertung

Erstellen Sie Benchmarks der aktuellen Active Directory-Konfiguration unter Berücksichtigung von vordefinierten Best Practices aus der Branche. Sie erhalten vollen Einblick in IOEs, IOCs und Tier-0-Assets. Dieses Active Directory-Sicherheits-Tool trägt zur Abwehr von Bedrohungen bei und verkleinert zusätzlich die Angriffsfläche.

Vorteile:

- **Verringern Sie die Angriffsfläche, indem Sie Ihr AD anhand von branchenübliche Best Practices bewerten**
- **Vereinfachen Sie die AD-Sicherheit mit Transparenz, Kontrolle und dem Schutz kritischer Assets**
- **Verhindern Sie Abweichungen der AD-Konfiguration und stellen Sie sicher, dass Sie Angreifern einen Schritt voraus sind**
- **Vermeiden Sie Müdigkeit durch zu viele Warnmeldungen und identifizieren Sie echte Bedrohungen, indem Sie sich auf die wichtigsten Warnmeldungen konzentrieren**
- **Verknüpfen Sie IOC- und IOE-Sicherheitssignale, um eine schnelle Reaktion auf Bedrohungen zu gewährleisten**

Fokus auf wichtige Assets

Identifizieren und priorisieren Sie mühelos Tier-0-Assets und stellen Sie so sicher, dass Ihre angreifbarsten Komponenten die höchste Aufmerksamkeit erhalten. Verschaffen Sie sich volle Kontrolle über diese kritischen Assets, indem Sie die Tier-0-Liste dynamisch anpassen, sodass sie immer auf die sich ändernden Anforderungen Ihres Unternehmens abgestimmt ist.

AD-Bedrohungsabwehr

Schützen Sie kritische AD-Objekte vor Kompromittierung und Fehlkonfigurationen, einschließlich sensibler GPOs. Dieses Sicherheits-Tool für Active Directory ermöglicht die Erstellung spezieller Berichte zum Objektstatus, die Ihnen den nötigen Kontext liefern, um geeignete Maßnahmen zu ergreifen.

AD-Bedrohungserkennung

Mit diesem Sicherheits-Tool für Active Directory können Sie Ihre Ziele bei der Abwehr von Bedrohungen stets im Auge behalten, indem Sie kontinuierlich nach IOCs und Konfigurationsabweichungen suchen und so sicherstellen, dass Sie für eine schnelle Reaktion auf potenzielle Sicherheitsvorfälle gut vorbereitet sind.

Schnelle Reaktion auf Vorfälle

Erfassen Sie das „Wer, Was, Wo, Wie und Wann“ von verdächtigen Aktivitäten mit intelligenten und kontextbezogenen Benachrichtigungen, die dazu beitragen, die Müdigkeit durch zu viele Warnmeldungen zu verringern. Leiten Sie IOEs und IOCs direkt an Ihre SIEM-Tools wie Microsoft Sentinel und Splunk weiter, um eine nahtlose Integration und zentrale Einblicke zu ermöglichen.

Vereinheitlichte Arbeitsumgebung für AD-Sicherheit

Konzentrieren Sie sich auf Ihr Kerngeschäft – mit einer benutzerfreundlichen Oberfläche, die nahtlos Einblick in IOEs, IOCs und andere Sicherheitssignale bietet.

> **Die Korrektur eines AD-Objekts, das unsachgemäß geändert wurde, kann Stunden dauern, und dadurch den Betrieb beeinträchtigen … Mit dem Objektschutz von Quest können wir verhindern, dass solche Probleme überhaupt erst entstehen.**
>
> *Allessandro Bottin, Global Infrastructure & Operation Manager, Prysmian Group*

Über Quest

Quest stellt Softwarelösungen bereit, mit denen das volle Potenzial neuer Technologien in einer zunehmend komplexen IT-Landschaft ausgeschöpft werden kann. Von der Datenbank- und Systemverwaltung über die Migration zu und Verwaltung von Active Directory und Microsoft 365 bis hin zur Cyber Resilience: Quest hilft Kunden, bereits heute ihre IT-Herausforderungen von morgen zu bewältigen. Quest Software. Where Next Meets Now.