IT Security Search

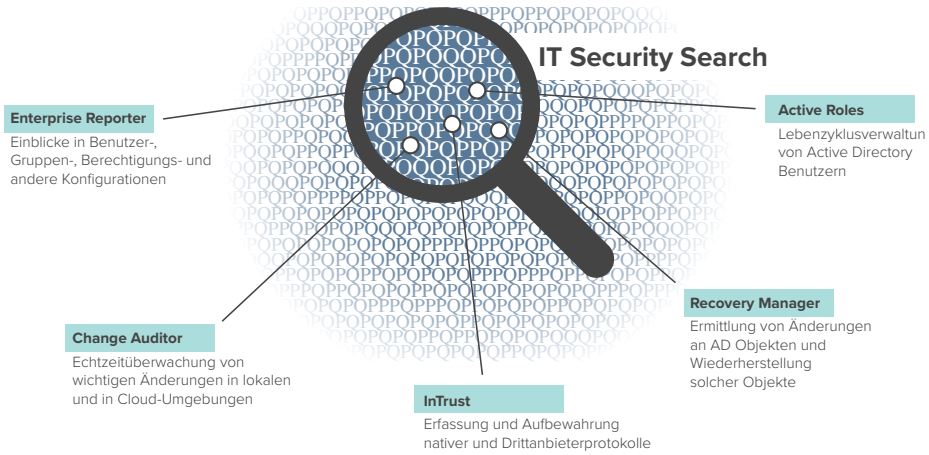
Korrelieren unterschiedlicher IT-Daten in einer interaktiven Suchmaschine

In einer heterogenen IT-Umgebung kann es schwierig sein, einen Überblick darüber zu behalten, welcher Benutzer Zugriff auf Daten hat, wie sie abgerufen wurden und wie dieser Zugriff verwendet wird. Die Extraktion von gut versteckten Informationen kann für die IT eine große Herausforderung darstellen. Es müssen Milliarden von Ereignissen aus verschiedensten Quellen erfasst und überprüft werden (lokal und in der Cloud), sodass es sich als extrem schwierig herausstellen kann, relevante Daten zu finden und aus diesen verwertbare Einblicke zu gewinnen. Im Fall einer internen oder externen Sicherheitslücke kann die Möglichkeit, die Quelle der Lücke und die betroffenen Informationen zu identifizieren, zudem einen großen Unterschied machen. Glücklicherweise ist dies mit IT Security Search, einer Funktion zahlreicher Quest® Lösungen, einfacher denn je.

IT Security Search ist eine Google-ähnliche IT-Such-Engine, mit der IT-Administratoren und Sicherheitsteams schnell auf Sicherheitsvorfälle reagieren und Ereignisforensik analysieren können. Über die webbasierte Oberfläche des Tools werden unterschiedliche IT-Daten aus verschiedenen Quest Sicherheits- und Compliance-Lösungen in einer zentralen Konsole korreliert.

Eine schnelle Suche verrät, wer was wann und wo gemacht hat – unabhängig davon, ob es sich dabei um eine Änderung wichtiger Active Directory (AD) Objekte, erweiterte Berechtigungen für einen Benutzer oder eine Gruppe oder den nicht autorisierten Zugriff auf vertrauliche Dateien oder Ordnerdaten handelt. Mithilfe von aussagekräftigen Darstellungen und Ereigniszeitleisten profitieren Sie zusätzlich von wertvollen Einblicken in die Verwaltung und die Stakeholder-Informationen.

IT Security Search ist als Bestandteil mehrerer Quest Lösungen verfügbar, darunter Enterprise Reporter, Change Auditor, InTrust®, Recovery Manager for AD und Active Roles; diese Komponente ruft Daten ab und führt sie in einer einzigen Anzeige zusammen. Dort können Sie sämtliche Aktivitäten in Ihrer lokalen oder hybriden Umgebung bequem prüfen und entsprechend reagieren. Konfigurieren Sie den rollenbasierten Zugriff, um Prüfern, Helpdesk-Mitarbeitern, IT-Managern und anderen Stakeholdern jeweils genau die Berichte bereitzustellen, die sie benötigen.



IT Security Search macht das Erkennen von internen und externen Sicherheitslücken einfacher als je zuvor.

IT Security Search verwendet eine einfache, natürliche Suchsprache, die es Administratoren und Sicherheitsteams ermöglicht, Insider-Angriffe schnell zu untersuchen.

VORTEILE:

- Vereinfachung der Suche nach sowie der Analyse und Aufbewahrung von wichtigen IT-Daten, die über mehrere Informationssilos verteilt sind
- Beschleunigung von sicherheitsbezogenen Untersuchungen und Compliance-Prüfungen dank eines lückenlosen Echtzeitüberblicks über privilegierte Benutzer und Server-/Dateidaten in einer einzigen durchsuchbaren Quelle
- Behebung weit verbreiteter Fehler im Falle eines Ausfalls oder einer Sicherheitslücke
- Einfache und schnelle Wiederherstellung beschädigter oder vorsätzlich geänderter AD Objekte
- Aktivierung eines rollenbasierten Zugriffs, um allen Stakeholdern jeweils genau die Berichte bereitzustellen, die sie benötigen

SYSTEMANFORDERUNGEN

KOMPATIBILITÄT

IT Security Search bietet Unterstützung für die folgenden Versionen von Systemen, die als Datenquelle fungieren können:

InTrust 11.4, 11.3.2, 11.3.1, 11.3, 11.2

Change Auditor 7.0, 6.9.5, 6.9.4, 6.9.3, 6.9.2, 6.9.1, 6.9, 6.8

Enterprise Reporter 3.1, 3.0, 2.6, 2.5.1

Recovery Manager for Active Directory 9.0.1, 9.0, 8.8.1, 8.8, 8.7.1, 8.7

Active Roles 7.3.1, 7.2.1, 7.2, 7.1, 7.0

SOFTWAREANFORDERUNGEN

Betriebssystem: Microsoft Windows Server 2016

Microsoft Windows Server 2012 R2

Microsoft Windows Server 2012

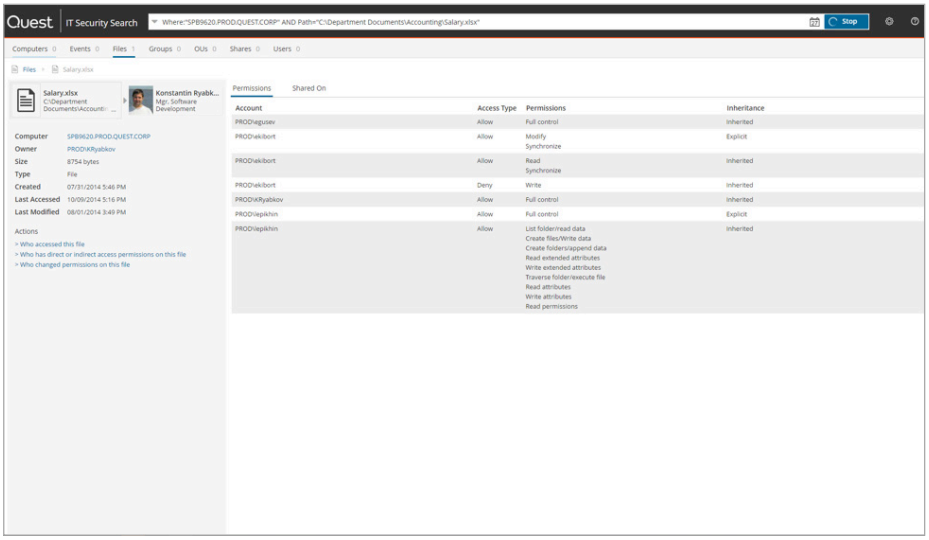
Microsoft Windows Server 2008 R2

Zusätzliche Software: Microsoft .NET Framework 4.6.2 oder höher

Microsoft Windows PowerShell 3.0 oder höher

Microsoft SQL Server 2012 oder höher (alle Editionen). Dies ist eine Anforderung der IT Security Search Warehouse Komponente (erforderlich für interne Konfigurationsverwaltung).

Eine vollständige Liste der aktuellen Systemanforderungen finden Sie unter quest.com/products/it-security-search.



Profitieren Sie von der lückenlosen Nachverfolgung des Benutzerzugriffs.

STATUSBASIERTE DATEN

- Mit Enterprise Reporter erhalten Sie in lokalen, Azure- und hybriden Umgebungen geschäftskritische Einblicke in Benutzer-, Computer- und Gruppeninformationen, direkte oder verschachtelte Gruppenmitgliedschaften, Ordnerberechtigungen auf Ebene der Organisationseinheiten (OE) und auf Dateiebene, Eigentümerschaft und mehr. Auf diese Weise können sich IT-Teams einen umfassenden Überblick über den Sicherheitsstatus verschaffen.
- Über Active Roles zeigen Sie virtuelle Attribute, dynamische Gruppenmitglieder, temporäre Gruppenmitglieder und verwaltete Einheiten an.

ÜBERWACHUNG DER SICHERHEIT IN ECHTZEIT

- Suchen Sie mit Change Auditor nach Echtzeit-Informationen über Änderungen an geschäftskritischen Objekten und vertraulichen Daten – ganz gleich, ob lokal oder in Office 365 und Azure AD.
- Zusätzlich zu den nativen Audit-Details erhalten Sie Informationen zum Benutzer, der die AD Änderung vorgenommen hat – und das auch bei Verwendung von Active Roles.

ERFASSUNG UND ARCHIVIERUNG VON PROTOKOLLEN

Mit der InTrust® Protokollverwaltung lassen sich native (Windows Server, Unix/Linux, Workstation und mehr) und Drittanbieterprotokolle aus Ihrem gesamten Unternehmensnetzwerk ganz einfach erfassen.

KOMPRIMIERTES, INDIZIERTES ONLINE-REPOSITORY

Über InTrust können Sie Volltextsuchen in Langzeit-Ereignisprotokolldaten und anderen Serverdaten durchführen, wenn dies aus Compliance- und Sicherheitsgründen erforderlich ist, und sparen so wertvolle Zeit für die Suche nach Ereignissen.

WIEDERHERSTELLUNG VON OBJEKTEN

Ermitteln Sie, welche AD Objekte geändert wurden – einschließlich der Werte vor bzw. nach der Änderung – und stellen Sie sie dank Recovery Manager for AD mit ein paar Klicks wieder her.

ÜBER QUEST

Quest liefert Softwarelösungen für die ständig im Wandel befindliche Welt der Unternehmens-IT. Wir helfen, die durch Datenexplosion, Cloud-Erweiterung, Hybrid-Rechenzentren, Sicherheitsbedrohungen und gesetzliche Bestimmungen hervorgerufenen Schwierigkeiten zu verringern. Unser Portfolio beinhaltet Lösungen für Datenbankverwaltung, Datenschutz, vereinheitlichte Endpunktverwaltung, Identitäts- und Zugriffsverwaltung sowie Verwaltung von Microsoft-Plattformen.

Quest
quest.com/de
Sie finden Informationen zu lokalen Niederlassungen auf (quest.com/de-de/locations)

DataSheet-ITSS-US-KS-DE-WL-38937