IT Security Search

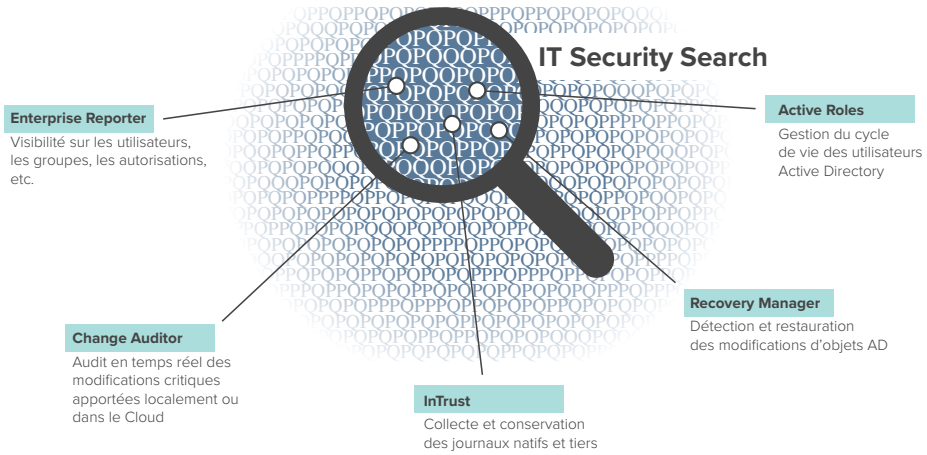
Corrélez les données informatiques disparates dans un moteur de recherche interactif

Il est parfois difficile de savoir qui a accès aux données, comment ces données ont été obtenues et comment l'accès est utilisé dans un environnement informatique disparate. Voir l'invisible peut être un véritable défi pour l'équipe informatique. Avec des milliards d'événements issus de diverses sources à collecter et à analyser sur site et dans le Cloud, il est difficile de trouver des données pertinentes et de les exploiter efficacement. En cas de faille de sécurité, interne ou externe, la faculté à identifier le point d'origine de la faille ainsi que les ressources qui ont été touchées peut faire toute la différence. C'est désormais chose aisée grâce à IT Security Search, une fonctionnalité commune à plusieurs solutions Quest®.

IT Security Search est un moteur de recherche semblable à Google qui permet aux administrateurs informatiques et aux équipes chargées de la sécurité de répondre rapidement aux incidents et d'analyser les événements en détail. L'interface Web de l'outil centralise les données informatiques disparates issues de plusieurs solutions Quest de sécurité et de conformité dans une console unique.

Une recherche rapide suffit pour découvrir qui a fait quoi, quand et où, qu'il s'agisse d'une modification d'objets Active Directory (AD) critiques, de privilèges élevés accordés à un utilisateur ou à un groupe, ou de l'accès inapproprié à des données de dossiers ou de fichiers sensibles. En outre, des affichages enrichis et des chronologies d'événements fournissent encore plus d'informations utiles à l'équipe de direction et aux parties prenantes.

IT Security Search est disponible en tant que composant de plusieurs solutions Quest, notamment Enterprise Reporter, Change Auditor, InTrust®, Recovery Manager for AD et Active Roles. Elle centralise les données et les flux au sein d'une console à partir de laquelle vous pouvez facilement identifier toutes les activités au sein de votre environnement hybride ou sur site et prendre des mesures en conséquence. Configurez l'accès basé sur les rôles pour permettre aux auditeurs, au personnel de support en ligne, aux responsables informatiques et aux autres parties prenantes d'obtenir exactement les rapports dont ils ont besoin et rien de plus.



IT Security Search simplifie l'identification des failles de sécurité internes et externes.

IT Security Search utilise un langage de recherche simple et naturel aidant les administrateurs et les équipes chargées de la sécurité à enquêter rapidement sur les attaques provenant de l'intérieur.

AVANTAGES :

- Simplification de la recherche, de l'analyse et de la maintenance des données informatiques critiques dispersées dans différents silos d'information
- Accélération des analyses de sécurité et des audits de conformité avec une visibilité en temps réel de vos utilisateurs à privilèges et des données des serveurs/fichiers dans un même emplacement interrogeable
- Dépannage des problèmes courants en cas de panne ou d'incident de sécurité
- Restauration simple et rapide des objets AD altérés ou modifiés du fait d'un acte de malveillance
- Accès basé sur les rôles pour fournir à toutes les parties prenantes les rapports dont ils ont exactement besoin et rien de plus

CONFIGURATION SYSTÈME REQUISE

COMPATIBILITÉ

Les versions suivantes des systèmes générant des données sont prises en charge par cette version d'IT Security Search :

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

CONFIGURATION LOGICIELLE REQUISE

Système d'exploitation : Microsoft Windows Server 2016

Microsoft Windows Server 2012 R2

Microsoft Windows Server 2012

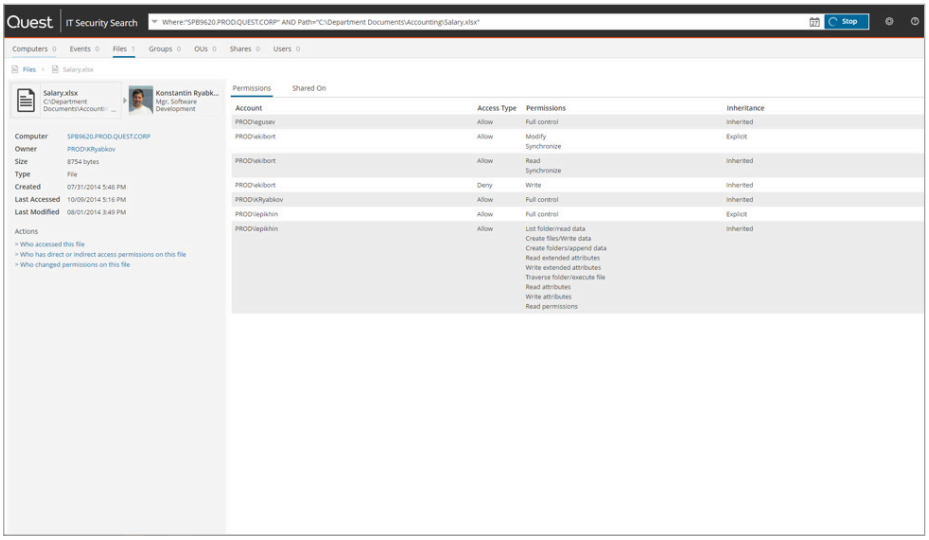
Microsoft Windows Server 2008 R2

Logiciels supplémentaires : Microsoft .NET Framework 4.6.2 ou version ultérieure

Microsoft Windows PowerShell 3.0 ou version ultérieure

Microsoft SQL Server 2012 ou version ultérieure (toutes les éditions). Il s'agit d'une exigence du composant IT Security Search Warehouse requise pour la gestion de la configuration interne.

Pour obtenir la liste détaillée et à jour des configurations requises, consultez le site quest.com/products/it-security-search.



Découvrez rapidement quel utilisateur a eu accès aux fichiers, pour quel motif, depuis quel emplacement et de quelle manière.

DONNÉES BASÉES SUR L'ÉTAT

- Obtenez des informations stratégiques sur les utilisateurs, les ordinateurs, les groupes, les adhésions aux groupes directes et imbriquées, les permissions des unités organisationnelles (UO) et des fichiers/dossiers, la propriété et bien plus dans les environnements sur site, Azure et hybrides avec Enterprise Reporter. Les équipes informatiques bénéficient ainsi d'une vision complète de l'état de la sécurité.
- Visualisez les attributs virtuels, les membres de groupes dynamiques, les membres de groupes temporaires et les unités gérées avec Active Roles.

AUDITS DE SÉCURITÉ EN TEMPS RÉEL

- Recherchez des informations en temps réel sur les modifications apportées à des objets stratégiques et des données sensibles, sur site ou dans Office 365 et Azure AD, avec Change Auditor.
- Complétez les détails des audits natifs avec des informations sur l'utilisateur ayant initié un changement dans AD, même si ce changement a été opéré depuis Active Roles.

JOURNAUX DE COLLECTE ET D'ARCHIVAGE

Rassemblez les journaux natifs (serveur Windows, Unix/Linux, station de travail, etc.) et les journaux tiers au sein du réseau hétérogène de votre entreprise avec la gestion des journaux assurée par InTrust®.

ESPACE DE STOCKAGE EN LIGNE INDEXÉ ET COMPRESSÉ

Effectuez des recherches en texte intégral sur des données de journal des événements à long terme et d'autres données de serveur à des fins de conformité et de sécurité avec InTrust, et gagnez du temps sur la recherche d'événements.

RESTAURATION D'OBJETS

Découvrez quels objets AD ont changé, avec notamment les valeurs avant et après, et restaurez-les en quelques clics avec Recovery Manager for AD.

PROFIL DE QUEST

Quest fournit des solutions logicielles adaptées au monde de l'informatique d'entreprise en rapide évolution. Nous simplifions les défis associés à l'explosion des données, à l'expansion dans le Cloud, aux datacenters hybrides, aux menaces de sécurité et aux exigences de conformité. Notre gamme de solutions couvre la gestion des bases de données, la protection des données, la gestion unifiée des terminaux, la gestion des accès et des identités, ainsi que la gestion des plateformes Microsoft.

Quest
quest.com/fr
Rendez-vous sur (quest.com/fr-fr/locations) pour obtenir les coordonnées de notre bureau local.

DataSheet-ITSS-US-KS-FR-WL-38937