IT Security Search

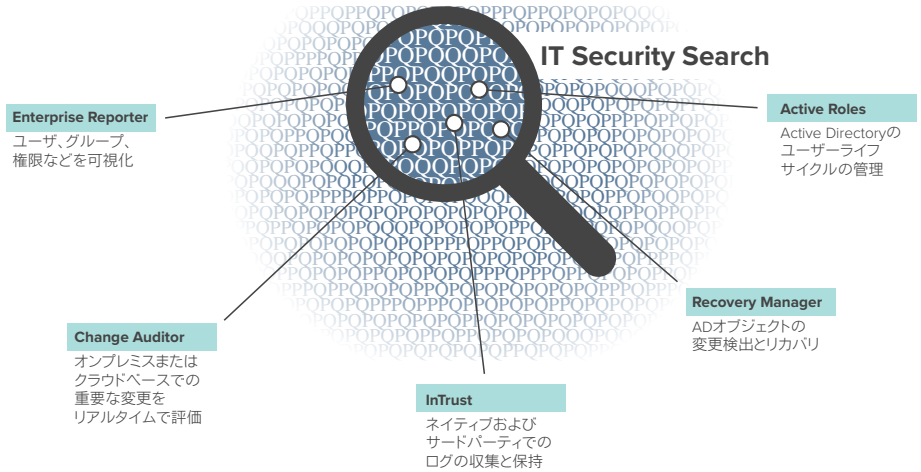
分散したITデータをインタラクティブな検索エンジンに関連付ける

誰がデータにアクセスできるのか、データをどのように取得し、そのアクセスをどのように使用しているのかを追跡することは、分散したIT環境では困難な場合があります。目に見えないものを見えるようにすることは、ITにとって挑戦と言えるでしょう。オンプレミスとクラウドのさまざまなソースから何十億ものイベントを収集して確認する必要があるため、関連するデータを見つけてその意味を理解するのは大変なことです。また、システム内外でセキュリティ侵害が発生した場合、侵入ルートやアクセスされたデータを特定できるかどうかで結果が大きく変わります。ですが、ご安心ください。いくつかのQuest®ソリューションの機能の1つであるIT Security Searchを使用すると、この作業をこれまで以上に簡単に行うことができます。

IT Security SearchはGoogleのようなIT検索エンジンです。IT管理者やセキュリティチームによる、セキュリティインシデントへの迅速な対応とイベントフォレンジックの分析を可能にします。このツールのWebベースのインターフェイスは、多くのQuestセキュリティ&コンプライアンスソリューションからの多様なITデータを単一のコンソールで関連付けます。

クイック検索機能を使用して、インシデントが誰によって、いつどこで行われたか、それがアクティブディレクトリ（AD）の重要なオブジェクトに対する変更であるか、ユーザまたはグループに昇格された特権が付与されたのか、または機密ファイルやフォルダデータに誰かが不正にアクセスしているのかを探り出すことができます。また、可視化の強化とイベントタイムラインの追加によって、管理者およびステークホルダーにより有益な情報を提供することができます。

Enterprise Reporter、Change Auditor、InTrust®、Recovery Manager for AD、Active RolesなどのQuestソリューションの一部として利用できるIT Security Searchは、データを抽出して1つのコンソールに表示します。その画面から、オンプレミスまたはハイブリッド環境におけるすべてのアクティビティを確認し、対処することが簡単にできます。監査担当者、ヘルプデスクのスタッフ、IT管理者などのステークホルダーに必要なレポートを厳密に過不足なく提供できるように、ロールベースのアクセスを設定できます。



IT Security Searchでは、システム内外でのセキュリティ侵害の識別がこれまでよりも簡単になります。

IT Security Searchは、管理者やセキュリティチームが内部からの攻撃を迅速に調査できるように、シンプルな自然言語の検索語句を使用します。

メリット:

- 情報のサイロ間で分散した重要なITデータの検索、分析、維持にまつわる複雑さを低減する
- 検索可能な1つの場所で、特権ユーザとサーバ/ファイルデータを完全にリアルタイムで見えるようにすることで、セキュリティ調査とコンプライアンス監査をスピードアップする
- アウテージやセキュリティ侵害が生じる問題のトラブルシューティングを広範囲にわたって行う
- 破損したか、または悪意を持って変更されたADオブジェクトを簡単かつ迅速に復元する
- ロールベースのアクセス設定により、各ステークホルダーに必要なレポートを厳密に過不足なく提供する

システム要件

互換性

このバージョンのIT Security Searchでサポートしているデータ提供システムのバージョンは、以下の通りです。

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

ソフトウェア要件

オペレーティングシステム: Microsoft Windows Server 2016

Microsoft Windows Server 2012 R2

Microsoft Windows Server 2012

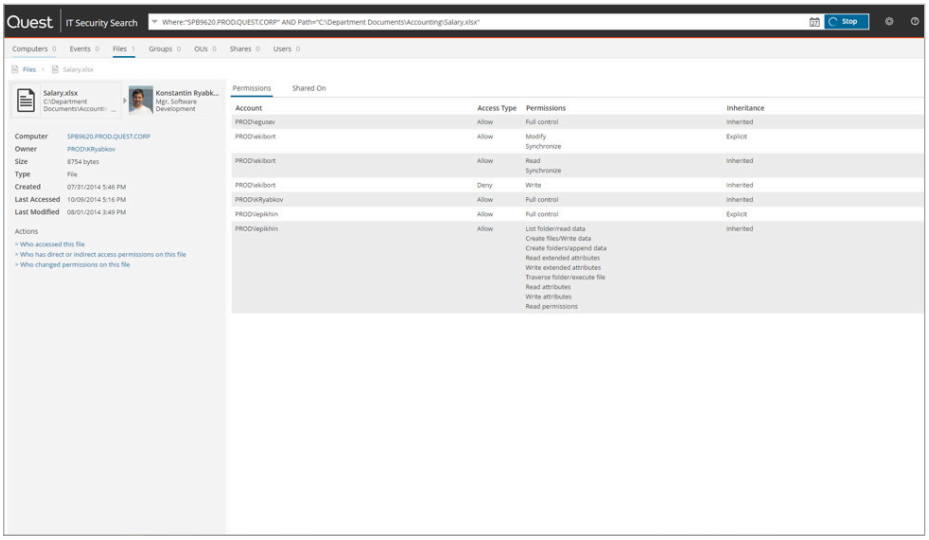
Microsoft Windows Server 2008 R2

追加ソフトウェア: Microsoft .NET Framework 4.6.2以降

Microsoft Windows PowerShell 3.0以降

Microsoft SQL Server 2012以降（すべてのエディション）。これは、内部構成管理のために必要なIT Security Search Warehouseコンポーネントの要件です。

最新のシステム要件の詳細な一覧については、quest.com/products/it-security-searchをご覧ください。



ユーザアクセスに関して、「誰が、何を、どこで、どのように」実行したかを容易に把握できます。

状態ベースのデータ

- ユーザ、コンピュータおよびグループ情報、直接およびネストされたグループメンバーシップ、組織単位（OU）およびファイル/フォルダのアクセス許可、所有権などに関する重要な情報を、オンプレミス、Azureおよびハイブリッド環境全体でEnterprise Reporterを使用して把握します。セキュリティの状態を包括的に理解できるよう、ITチームを強化します。
- Active Rolesの仮想属性、動的グループのメンバー、一時グループのメンバー、管理ユニットを表示します。

リアルタイムセキュリティ監査

- オンプレミスかOffice 365やAzure ADかを問わず、重要なオブジェクトや機密データへの変更に関する情報を、Change Auditorを使用してリアルタイムで検索します。
- Active Rolesを介して変更が開始された場合であっても、ADを実際に変更したユーザの情報をネイティブ監査データに付け加えます。

ログの収集とアーカイブ

ネイティブのログ（Windowsサーバ、UNIX/Linux、ワークステーションなど）だけでなく、さまざまな企業ネットワーク上にあるサードパーティのログも、InTrust®のログ管理を使用して収集します。

圧縮率の高い、インデックス化したオンラインレポジトリ

コンプライアンスやセキュリティのために、InTrustを使用して長期間のイベント・ログ・データやその他のサーバデータでフルテキスト検索を行い、イベントの特定にかかる時間を削減することができます。

オブジェクトのリカバリ

Recovery Manager for ADを使用して、どのADオブジェクトが変更されたかを見つけ出し（変更前後の値を含む）、数回のクリックで復元します。

QUESTについて

Questは、急速に変化するエンタープライズITの世界にソフトウェアソリューションを提供しています。データの爆発、クラウドサービスへの拡張、ハイブリッドデータセンター、セキュリティ脅威、規制上の要件によって生じる課題のシンプル化を支援します。Questのポートフォリオは、データベース管理、データ保護、統合エンドポイント管理、IDおよびアクセス管理、Microsoftプラットフォーム管理などのソリューションで構成されます。

Quest
quest.com/jp
世界各地のオフィスの情報については、（quest.com/jp-ja/locations）をご覧ください

DataSheet-ITSS-US-KS-JA-WL-38937