Change Auditor for Logon Activity

ADのログオン/ログオフアクティビティとAzure ADのサインインアクティビティについて、警告およびレポート作成を行います

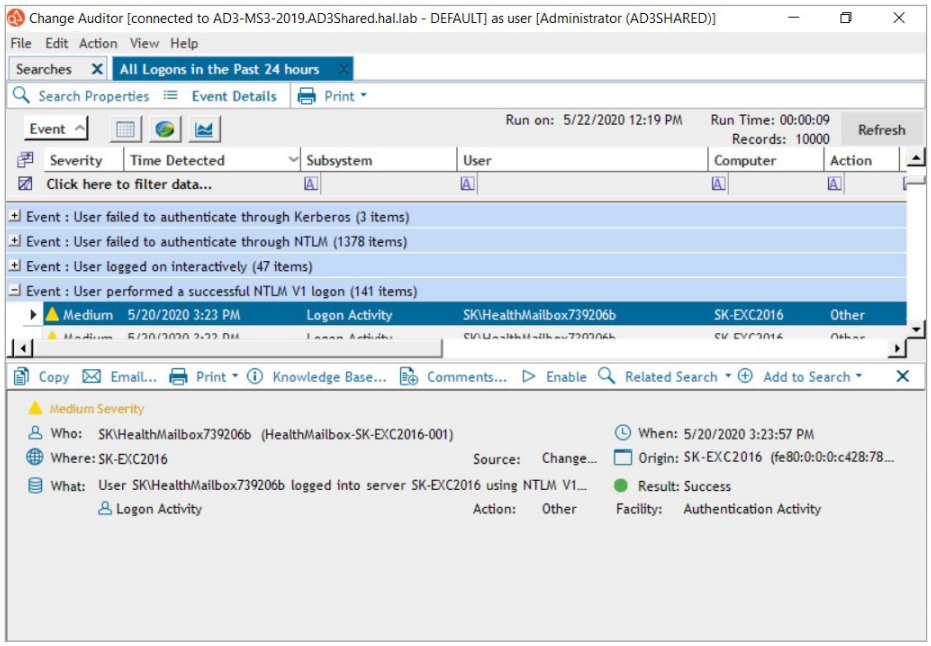
今日ではコンプライアンス規制やセキュリティの懸案事項が増加しており、ユーザのログオン/ログオフアクティビティを自動追跡できる、完全で信頼のおける機能が不可欠です。しかし、ほとんどのサードパーティ製ツールは導入するのが面倒で、オンプレミスでもクラウドサービスでも、ユーザアクションの十分な説明責任を保証するために必要なレベルの監査を行うことができません。一方、ネイティブツールには、可視性、アラート、監査、およびデータセキュリティにおいて重大な欠点があります。

Change Auditor for Logon Activityがあれば、ADのログオン/ログオフアクティビティとAzure ADのサインインアクティビティをキャプチャして警告やレポート作成を行うことで、組織のセキュリティ、監査、コンプライアンスを強化できます。また、Kerberos認証とNTLM認証の両方を追跡して、脆弱性をプロアクティブに識別できるようにします。

特長

ホステッドダッシュボード— 柔軟に検索でき、データが可視化されたSaaSダッシュボードのOn Demand Auditで、ADユーザのログオン/ログオフ、Azure ADのサインイン、およびOffice 365のアクティビティをすべて一緒に表示します。

一目で把握できる表示 — ユーザや管理者の重要なログオンアクティビティを追跡できます。誰が、何を、いつ、どこで、なぜ、どのワークステーションから実行したかなどを詳細に把握できます。



ハイブリッドログオン/ログオフおよびサインインアクティビティを追跡して、詳細なセッション情報を把握できます。データをグループ分け、ソート、フィルタして、リモートでログインしているユーザとその場所がわかります。

「何らかの問題がある場合、マネージャは何が変わったかに関するレポートを必ずIT部門に求めます。ネイティブツールでは、特にITスタッフに制限があるため、これらの要求に迅速に対応できませんでした。しかし、Change Auditorを使用すると、レポートをすぐに作成し始めることができます。これが私たちには本当に重要なことなのです。」

ハワード郡、サーバ・チーム・マネージャ、John Eckard氏

メリット:

- ADのログオン/ログオフアクティビティとAzure ADのサインインアクティビティをすべてキャプチャして警告し、レポートを作成
- Kerberos認証とNTLM認証の両方を追跡し、脆弱性の識別を支援
- セッション、ログオン/ログオフ、サインインアクティビティ（開始/終了時間を含む）、および変更イベントに関する重大な情報（実行者、内容、時間、場所、実行元/ワークステーション）についての企業全体における可視性を実現
- 複数かつ多様な、暗号化されたログオンイベントを自動収集
- セキュリティおよび監査を目的としたシンプルな統合レポート
- 現場にいないときでも、至急の対応を促すリアルタイムの警告をEメールやモバイルデバイスに送信
- 失敗したログオンについて警告することでセキュリティリスクを低減
- SIEMソリューションと統合して、Change AuditorイベントをSplunkやArcSight、QRadarに転送

システム要件

システム要件の詳細については、support.quest.com/technical-documents/change-auditorにある『Installation Guide（インストールガイド）』をご覧ください。

完璧なユーザアクティビティ監査 — ログオンからログオフ、そしてその間に実行するすべてのアクティビティ（他のChange Auditorモジュールと組み合わされた場合）にわたって、管理者アクティビティのタイムライン全体を監査します。

ゴールデンチケットの検知 — チケットゴールデンチケット/Pass-the-ticket攻撃中に使用される一般的なKerberos認証の脆弱性を検知して警告します。

NTLM認証の監査— 比較的にセキュアでないNTLM認証を使用し続けているアプリケーションを検知します。

コンプライアンスに対応したレポート作成 — ログオンアクティビティの収集をシンプル化して、社外の主要な規制や社内のセキュリティポリシー要件に準拠できるようになります。

移動中も可能なリアルタイム警告 — 成功したログオンと失敗したログオンの両方について、重要なアラートをEメールやモバイルデバイスで受け取ることができます。これにより、オフィスを離れていても、セキュリティの脅威に迅速に対応できます。

改善されたセキュリティインサイト — 分散したITデータを、多くのシステムやデバイスから、迅速なセキュリティ対応とフォレンジック分析を可能にするインタラクティブな検索エンジンであるIT Security Searchへと関連付けます。ユーザの資格とアクティビティ、イベントのトレンド、不審なパターンなど、さまざまなデータを豊富な可視化機能やイベントタイムラインを使用して確認できます。

ハイブリッド環境のセキュリティの把握 — ADユーザのログオン/ログオフについてレポートを作成し、Azure ADのサインインと関連付けて、ハイブリッドのクラウドサービス環境にわたる疑わしいアクティビティの識別を支援します。キャプチャされる情報には、ログオンの種類、IPアドレス、地理的な起源、認証されるアプリケーション、試みが成功したかどうかが含まれます。

関連付けられた検索 — 現在表示されているイベントに関するあらゆる情報と、関連するすべてのアクティビティを、ワンクリックで瞬時に把握できます。これにより、憶測に基づいた作業を減らし、セキュリティ上の懸案事項を明確化できます。

統合イベントの転送 — SIEMソリューションと簡単に統合でき、Change AuditorイベントをSplunkやArcSight、QRadarに転送できます。さらにChange AuditorはQuest® InTrust®と統合して、20:1に圧縮されたイベントストレージおよび一元化されたネイティブまたはサードパーティのログ収集、アラート機能による解析と分析、および不審なイベントに対する自動応答アクションを実現します。

ベストプラクティスのレポート作成 — ベストプラクティスへの準拠に役立つ包括的なレポート（アクセスレポート、ログオンの成功/失敗レポート、認証比較レポート、ユーザ別にグループ化されたレポートなど）が得られます。

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の管理、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-ChangeAuditorLogonActivity-US-AR-JA-WL-59222