Change Auditor for Active Directory

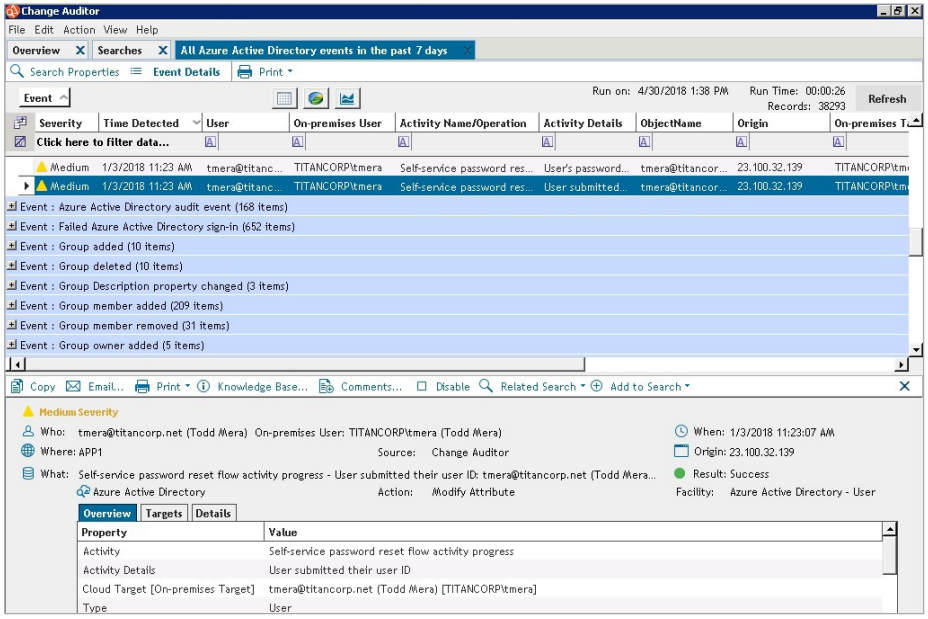
Active DirectoryおよびAzure Active Directoryのリアルタイム監査

Microsoft Active Directory（AD）は、ミッションクリティカルなネットワークインフラストラクチャの中核となるものです。ADに問題が発生すると、高いコストのかかる予期しないサービス中断が発生したり、ネットワークダウンタイムによってビジネスに支障が出たりすることがあります。危険を招くセキュリティデータ漏洩やSOX、PCI、HIPAA、GDPRなどの重大な政府規制への違反による莫大なコストについては言うまでもありません。組織にはADとAzure AD両方の重要な変更に関するリアルタイムの通知が必要です。

Quest® Change Auditor for Active Directoryは、ADとAzure ADのセキュリティと制御を促進するために、すべての重要な設定変更を追跡し、単一のコンソールに統合します。Change Auditorは、オンプレミスおよびクラウド環境に影響を及ぼす変更について追跡、監査、報告、および警告を行います。その際に、ネイティブの監査機能実行によるオーバーヘッドは生じません。Change Auditor for ADを使用すると、誰が、何を、いつ、どこで変更したか、どのワークステーションで変更が行われたかに関する情報を、関連するイベント詳細と共に取得できます（例: 変更前後の値や関連するオンプレミスおよびクラウドIDなど）。また、監査要件を満たすために特定の変更が行われた理由を説明するコメントを追加することもできます。Change Auditor for ADを使用すると、あらゆる重要な変更を素早く効率的に監査して、貴重なデータやリソースの安全性を確保できます。

重要な変更をすべて監査

ADおよびAzure ADのあらゆる重要な変更に関する広範かつカスタマイズ可能な監査



Change Auditor for Active Directoryを使用すると、誰が、何を、いつ、どこで変更したか、どのワークステーションで変更が行われたかに関する情報を時系列順に取得できます（関連するオンプレミスおよびクラウドIDなど）。

メリット:

- 数分程度でインストールでき、迅速なイベント収集でWindows環境を即座に分析
- 1つのクライアントで全社規模、オンプレミス、およびクラウドの監査とコンプライアンスが可能
- ユーザ行動パターンに基づいてプロアクティブに脅威を検知
- すべてのイベントおよび特定のインシデントに関する変更を追跡して未知のセキュリティの問題をなくし、アプリケーション、システム、およびユーザへの継続的なアクセスを確保
- 社内外のあらゆるデバイスにリアルタイムでアラートを送信して瞬時の対応を可能にし、セキュリティのリスクを数秒程度で低減
- 望ましくない変更の防止によって社内の制御を強化し、認定ユーザの制御権限を制限
- アカウントのロックアウトをプロアクティブにトラブルシューティングすることにより、可用性を向上
- ネイティブの監査機能を使用せずにイベントを収集することにより、サーバ上でのパフォーマンスの低下を抑えてストレージリソースを節約
- 企業のポリシーやGDPR、SOX、PCI DSS、HIPAA、FISMA、SAS 70など政府が定める規制法令へのコンプライアンスを合理化
- 情報に基づいて、監査人や経営陣に役立つインテリジェントで詳細なフォレンジックを実現

「全体的に見て、Change Auditorは非常に役立っています。当校が検討した製品の中で、Active Directoryのすべての変更に対してWindowsの監査機能を有効にする必要なく、これほどのレベルのリアルタイム監査と保護機能を提供するものは、他にありませんでした。」

Patrick Rohe氏
シニアITアーキテクト
タウソン大学

システム要件

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

およびレポートを取得できます（例えば、グループ・ポリシー・オブジェクト（GPO）、ドメイン・ネーム・システム（DNS）、サーバ構成、ネストされたグループ、その他多数に対して行われた変更）。ネイティブ監査と異なり、ADおよびAzure AD環境のオンプレミス、クラウド、およびハイブリッドADのすべての変更アクティビティが期間中のその他のイベントに関連する詳細なフォレンジックと共に時系列順に統合ビューに表示されます。また、プロアクティブなアラートを受け取ることができるため、常に状況を把握でき、重要なポリシー変更やセキュリティ侵害が発生すれば、場所やデバイスを問わずどこからでもそうした事態に対処して日常の変更に伴うリスクを軽減できます。

ユーザのアクティビティを追跡して望ましくない変更を防止

アカウントのロックアウトと重要なレジストリ設定へのアクセスに関するユーザと管理者のアクティビティを追跡することによって、全社規模の変更および制御ポリシー強化に役立ちます。重要な変更の発生を最初の段階でプロアクティブに制御し、24時間365日アラートを発行します。また、詳細な分析、変更前の値のリストア機能、およびレポート作成機能により、ADおよびAzure AD環境が不正アクセスを狙った疑わしい行動にさらされることを防止して、常に企業と政府規則が定める規則に準拠した状態を維持します。

CHANGE AUDITOR THREAT DETECTIONによるプロアクティブな脅威検知

異常なアクティビティを分析して組織におけるユーザのリスクをランク付けすることにより、ユーザ脅威の検知を簡素化し、潜在的な脅威を識別すると同時に、誤検知アラートによるノイズを削減します。

無関係なデータを意味のある情報に変換してセキュリティとコンプライアンスを促進

重要な変更を追跡し、生データを意味のある情報へと変換することで、お客様のインフラのセキュリティとコンプライアンスを保ちます。Change Auditor for ADを使用すると、誰が、何を、いつ、どこで変更したか、どのワークステーションで変更が行われたかに関する情報を、関連するイベント詳細（例: 変更前後の値）と共に取得できます。したがって、素早くセキュリティ関連の意思決定を行えます。また、Change Auditorの高性能な監査エンジンを使用すれば、監査の制限がなくなります。ネイティブ監査ログを必要とせずに、より短時間で結果が得られ、ストレージを節約できます。

統合イベント転送

SIEMソリューションと容易に統合し、Change AuditorイベントをSplunk、Micro Focus ArcSight、またはIBM QRadarに転送できます。さらに、Change Auditorは、Quest® InTrust®と統合して、20対1に圧縮された長期的なイベントストレージとネイティブまたはサードパーティによるログの集約を実現することで、SIEM転送におけるストレージコストを削減し、高圧縮のログリポジトリを作成します。

企業と政府の規制に合わせてレポート作成を自動化

Microsoft SQL Server Reporting Servicesを使用して、整理された、意味のあるセキュリティおよびコンプライアンスレポートを素早く取得できます。組み込みのコンプライアンスライブラリとカスタマイズ可能なレポートを使用すれば、GDPR、SOX、HIPAA、PCI DSS、FISMA、SAS 70などの政府の規制へのコンプライアンスの証明は極めて容易です。

QUESTについて

Questでは、複雑な問題をシンプルなソリューションで解決することを目的としています。当社は、優れた製品と優れたサービスを大切にし、シンプルにビジネスを行うという全体的な目標を重視する哲学をもって、これを達成しています。当社のビジョンは、効率性と有効性のどちらも犠牲にしないテクノロジーを提供することです。これにより、お客様と組織はIT管理の時間を短縮し、より多くの時間をビジネスの革新に費やすことができます。

Quest
国内外のオフィスの情報については、当社のWebサイト（Quest.com/jp）をご覧ください。

DataSheet-ChangeAuditor4AD-US-KS-JA-WL-33959