Change Auditor Threat Detection

Microsoft環境におけるユーザ脅威のプロアクティブな検知

大多数の組織が認証と認可を主にActive Directory（AD）に依存していることから、ADはハッカー、サイバーテロリスト、そして会社に不満をもつ元従業員から最も狙われる標的となっています。しかし、そのADのセキュリティに対するより直接的な脅威は、実は内部者の意図的な、あるいは意図しない行動であることに、どれだけの組織が気づいているでしょう。さらに、ADそのものの複雑性が、実際に脅威が発生した際の識別を、非常に困難なものにしています。また、ユーザ脅威を検知する従来のルールベースの手法では、発生する警告があまりにも多すぎて、すべてを調査することはとてもできません。つまり、そこに隠れている真の脅威を見逃してしまうおそれがあり、組織はデータセキュリティ侵害のリスクにさらされたままになるのです。では、どうすれば組織環境で起きているユーザのアクティビティをすべてリアルタイムに分析し、業務を混乱や停止から保護することができるのでしょうか?

Change Auditor Threat Detectionは、ユーザ個々の行動パターンをモデル化するという独自のユーザ脅威検知手法を使って、不審なユーザや乗っ取られたアカウントの兆候となる異常なアクティビティを検知します。独自の先進的な学習テクノロジーであるユーザおよびエンティティ行動分析（UEBA）と精緻な点数化アルゴリズムを使用したユーザアクティビティの分析により、Change Auditor Threat Detectionは組織内で高いリスクを有するユーザをランク付けし、潜在的なユーザ脅威を識別すると同時に、誤検知によるノイズを削減します。それにより、従来の監査ツールの欠点が克服され、セキュアな組織環境を維持することができるようになります。

特長

リアルタイム監査ログ分析

ADの変更、認証、ファイルに対するアクティビティなど大量の監査データを、リア

Change Auditor Threat Detectionを使用することで、不審なユーザアクティビティを迅速かつ容易に検知できるようになり、組織環境とユーザをセキュアに保つことができます。

メリット:

- ユーザの行動パターンに基づいて、脅威をプロアクティブに検知
- ルールベースの脅威検知にはつきものの膨大な警告を削減
- セキュリティ警告の重要度を迅速かつ容易に判断できるよう、警告をコンテキストと共に表示
- ユーザ行動ベースラインを使用して、ユーザの異常な行動を容易に検知
- 既存の監査データに基づいて脅威を識別し、インフラストラクチャへの影響を最小化

使用例:

Change Auditor Threat Detectionを使用して、次のような脅威を迅速かつ容易に検出できます。

- 異常なADアクティビティ
- 特権アカウントの悪用
- 総当たり攻撃
- データの外部持ち出し
- システムまたはリソースへの不適切なアクセス
- マルウェア
- 権限昇格
- ラテラルムーブメント

システム要件

CHANGE AUDITOR COORDINATOR

（サーバ側コンポーネント）

プロセッサー: クアッドコアインテル® Core™ i7（または同等以上）

メモリ: 8 GB RAM（最小）、32 GB RAM以上（推奨）

CHANGE AUDITOR CLIENT

（クライアント側コンポーネント）

プロセッサー: デュアルコアインテル® Core™ i5（または同等以上）

メモリ: 4 GB RAM（最小）、8 GB RAM以上（推奨）

CHANGE AUDITOR AGENT

（サーバ側コンポーネント）

プロセッサー: デュアルコアインテル® Core™ i5（または同等以上）

メモリ: 4 GB RAM（最小）、8 GB RAM以上（推奨）

詳細かつ最新のシステム要件リストについては、support.quest.com/change-auditorを参照してください。

ルタイムで、効率的に分析します。これら無加工のアクティビティイベントからユーザベースラインを構築し、ユーザの行動がそこからはずれた際にプロアクティブな検知を行うため、不審なアクティビティがあればただちに気づくことができます。

自動ユーザ行動分析（UEBA）

管理者がいっさい入力や設定をすることなしに、ユーザアクティビティのパターンをモデル化します。ユーザ行動ベースラインは、教師なしの高度な機械学習を使用して自動的に作成され、ログオンのパターン、管理アクティビティ、ファイルやフォルダへのアクセスなど、あらゆるユーザアクティビティについてモデル化します。

精緻な異常行動検知

ユーザの行動を自動で逐一ユーザ行動ベースラインと照らし合わせ、異常なユーザアクティビティを識別します。精緻な脅威兆候検知とマルチレベルのリスク点数化により、重大な異常のみがハイライトされ、真にリスクの高いユーザ行動として表示されます。

パターンベースのユーザ脅威検知

SMARTユーザ脅威警告は、異常なユーザ行動の相関パターンが検知されたときにのみ発生します。ルールに照らして特定のアクティビティを検知するのではなく、自動的にすべてのユーザアクティビティを発生と同時に分析し、精緻なユーザ行動パターン検知によりその組織環境において最も不審なユーザを識別します。精緻なグローバルモデリングにより、最も危険で対応を要するユーザ行動のみがハイライトされるため、関連性のない個々のアクティビティや誤検知によるノイズを大幅に削減できます。

忠実度の高いユーザ分析

Change Auditorは分析に使う監査ログを作成しますが、組織環境における脅威のプロアクティブ検知に使用されるこの未加工のイベントデータには、もともと以下のような有用な情報が含まれています。

- 誰が変更したか
- 何を変更したか
- いつ変更したか
- どこで変更したか
- 変更操作を行ったマシンのIPアドレスまたはワークステーション名

Windowsに組み込みのイベントログとは異なり、Change Auditorのログには、それがないとユーザ行動分析に致命的な差異が生ずるような重要なユーザ行動は、確実に含まれるようになっています。

コンテキストが明確なセキュリティ警告

不審なユーザアクティビティについての警告はすべて、発見された脅威の兆候のコンテキストと共に表示されます。異常行動はすべて、ユーザのベースラインアクティビティのコンテキストと照合し、警告のトリガとなったすべての未加工のイベントと共に表示されます。これにより、警告の発生理由が明確になり、調査とフォローアップが容易になります。

手軽なユーザ脅威検知

既存のChange Auditorインフラストラクチャと監査データを活用してユーザ行動をモデル化するので、余分な手間がかかるエージェントやサーバを追加せずにすみます。仮想アプライアンスを1つインフラストラクチャに追加するのみで、高度なユーザ脅威分析が可能となります。

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、効率か効果かの択一を迫らないテクノロジーを提供することです。これにより、お客様はIT管理に費やす時間を短縮し、より多くの時間をビジネスの革新に使うことが可能になります。

DataSheet-ChangeAuditorThreatDetection-US-KS-JA-WL-32855