ソリューション概要

顧客事例：エンタープライズ SaaS のための行動アナリティクス

メリット

- 俊敏なアクセス管理により業務プロセスを実施
- 誰がどのように機密データにアクセスしたのかを確実に把握
- 内部の不正行為やID情報への不正アクセスに対する不安を排除
- 実際の脅威への対応に関するレスポンスやガバナンスに注力

ビジネスの敏捷性とスピードを実現しながら確実性を強化

競争の激しい今日の市場において、スピード、俊敏性、情報へのアクセス性、そして迅速な決断を下すための信頼できるデータがあるかどうかということが、成功する企業と競争から脱落する企業の差を生みます。従来のセキュリティエンゲージメントモデルでは、業務要件を満たす安全なシステムの導入に焦点が当てられていますが、稼働開始後に市場のニーズが急速に変化した場合、どれほど俊敏なセキュリティチームであっても能力を超える作業負荷がかかり、セキュリティ部門と業務部門の間には緊張関係が生じることになります。

それでは、セキュリティチームはどうすれば必要最低限の権限と目的を与える「役割ベースのアクセスコントロール」（RBAC）の原則に従いながら、ビジネスの自然な変化に対処できるのでしょうか。

Informatica Secure@Sourceのユーザー行動アナリティクス（UBA）機能を使用することで、IT管理者が長年親しんできたアクセスコンプライアンスモデルを適用し、データを誰がどのように使用しているかを確実に把握して、データ所有者にインサイトを提供することができます。UBAをアラートやレスポンスと組み合わせることで、データの管理者と所有者は、ID情報への不正アクセスや権限の乱用による固有リスクを管理し、軽減できます。

UBAは監査チームやコンプライアンスチームが使い慣れているモデルを提供するので、厳格な規制環境であっても、セキュリティ態勢に影響を及ぼすことなく、競争力を維持するために必要な情報へ迅速にアクセスすることができます。

適切な権限を持つユーザーのリスクを正確に数値化

状況と機会

ビジネスの変化が急速な環境では、セキュリティとアクセスへの不安が変化のスピードを鈍らせ、ビジネスの推進が妨げられる場合があります。この場合、企業は次善の策としてメインの管理システムの外部でデータ管理やアナリティクスなどを実行することもあり得ます。

その結果として生じる無秩序なアクセスコントロールは管理が非常に難しく、どのデータセットに誰がアクセスできるのかが分かりにくいため、誤用や乱用の検出が不可能になります。業務プロセスがデータをどのように使用したり提供したりするのかを把握することは、業務トランザクションを中断させることなくコントロールを改善するための基盤となります。

スピードと俊敏性に対する企業のニーズ、確実なデータアクセスに対する規制上の要件、コンプライアンス推進者の保守的立場へのニーズなどが合わさることで、ユーザーがどのデータにアクセスできるかだけでなく、データで何をするのかという点も確実に管理できる機能への機会が創出されます。

インフォマティカについて

デジタルトランスフォーメーションによって世界が変化しています。エンタープライズクラウドデータ管理のリーダーであるインフォマティカは、時代をインテリジェントにリードする企業を万全の態勢でサポートすると共に、俊敏性を高め、新たな成長機会を実現するだけでなく、新たなモノを生み出すことさえ可能にする将来への洞察力を提供します。インフォマティカは、企業がこれからのインテリジェントな破壊的イノベーションを推進できるよう、当社が提供するあらゆるサービスを通じてデータの力を継続的に引き出すことを支援します。

アプローチとソリューション

UBAは、ビジネスのスピードと柔軟性を維持しながら、データアクセスに求められる確実性も提供します。インフォマティカ社内の例では、最初にいくつかの重要な業務プロセスを検証し、対象のデータセットが信頼できるソースからアナリティクス／レポーティングスタックを通って下流へ移動するまでを追跡しました。単一アプリケーション内だけでなく、データドメイン全体のアクティビティを評価することで、データセットのアクティビティに関する幅広いコンテキストを提供し、データ利用の制限に関する確実性を強化できます。事前にユーザーアクセスのシナリオは定義しておらず、代わりに異常検出やレポート機能によってユーザーアクションを監視することで、確実性とアカウンタビリティを確保しました。

検出やアラートだけでリスクを軽減することはできません。ユーザー、データ所有者、管理者の迅速なアクションが必要です。データ所有者とチームマネージャーは、早い段階でこの輪に組み入れる必要があります。データ所有者とチームマネージャーは、データへのアクセスによって生じるリスクについて結果責任を負う必要があります。これは、データの観点からリスク（または潜在的リスク）を示す方法が一番です。多くの場合、データの所有者やマネージャーは、データアクセスや利用パターンについて、簡単に活用できるインサイトを有していません。ユーザー、管理者、データ所有者が参加するフィードバックループでは、使用パターンや許容可能な行動が重視され、責任あるパターンの採用が推奨されます。

「非常時（Break-glass）」アクセスモデルとこのモデルの間には多くの類似点があります。「非常時（Break-glass）」アクセスモデルとは、通常は保守やトラブルシューティングの際に職務分離の制限を違反する必要のある、機密性の高いシステムの管理者が使用するものです。管理者は、この役割の機能を果たすための適切な権限を有しています。アクセスのレベルが上がると、すべてのアクションが承認されていることを確認するための検証が実行されます。監査担当者が妥当性を認めた場合、機械学習を使用することでこのモデルを拡張し、組織全体をカバーできるようになります。

質の高いプログラムを作成するには、最初にアクション指向のレスポンスモデルの最適化に焦点を当て、ユーザーの挙動や異常へ対応できるようにする必要があります。次に、スピードと俊敏性を必要とする業務プロセスまたは自社の目標に重大なリスクをもたらす業務プロセスへ対応できるように拡張します。

結論

Secure@Sourceの機械学習機能は、手作業による検証では達成できないレベルの確実性を提供し、データの用途に適したアクセス権が付与されるようになります。

UBAはデータ所有者モデルを統合して正式な推進者を確立し、所有者によるデータの管理と保護を促進します。認識プログラム、対象を絞ったトレーニング、またプロセスの改善措置を通して、UBAはプロセスの改善と変更を促進し、企業が急速に成長しながらコンプライアンスの目標に従うように支援します。

UBAは特定のアプリケーションやプラットフォームに縛られないため、さまざまなアプリケーションにまたがって使用することで、例えばソースシステムのみに注力してレポートシステムは対象外にするといったような事態を回避し、データエコシステム全体を保護することができます。

インフォマティカのSecure@Source UBAは、データ所有者と管理者をレスポンスプロセスに関与させることで、ビジネスのスピードと俊敏性をサポートするとともに、セキュリティとコンプライアンスの目標達成を支援します。

Informatica

〒105-6226 東京都港区愛宕2-5-1 愛宕グリーンヒルズMORIタワー26階 電話：03-6403-7600(代表) FAX：03-3433-1021
www.informatica.com/jp linkedin.com/company/informatica twitter.com/Informatica

IN17_0617_3339