DATA SHEET

CA Threat Analytics for PAM

概要

特権アカウントの悪用または奪取は、現在最も共通の脅威です。CA Threat Analytics for PAM では、継続的でインテリジェントな監視機能が提供されるため、企業は被害が発生する前にハッカーや悪意のある内部関係者を**検出**して**停止**できます。このソフトウェアによって、CA Privileged Access Manager（CA PAM）の信頼できる制御機能に強力なユーザ動作分析と機械学習アルゴリズムが統合されます。その結果、個々のユーザーの活動を継続的に分析して、リスクの高い不正な活動を正確に検出し、緩和策を自動的にトリガして企業への被害を制限するソリューションが実現します。

主なメリット / 成果

- **リスクの軽減：**高度な動作分析で攻撃を検出して回避できます。
- **意味のある洞察：**インシデント対応とコンプライアンスが簡略化されます。
- **即時の価値提供：**検出機能、優れたユーザ・エクスペリエンス、および洞察が導入後すぐに提供されます。
- **特別なスキルが不要：**アルゴリズム、データ・サイエンス、機械学習の専門知識は必要ありません。

主な特長

- **高度な脅威分析：**クレジット・カード詐欺を撃退するために銀行が使用している動作分析の手法（機械学習のアルゴリズムによるアクティビティの履歴分析とリアルタイム分析、リスク評価、緩和策のトリガ）を使用してデータを保護できます。
- **攻撃とリスクの自動検出:**自動分析を使用して、攻撃、リスクの高いアクティビティ、および侵害をすばやく検出する継続的な監視機能が提供されます。
- **対応と緩和：**セッション記録やステップアップ認証などの緩和策が自動的にドリガされるため、内部関係者や攻撃者の侵入を防止できます。
- **既存のシステムの強化：**統合されたアドオンとして、コンテキスト・リッチ・アラートとレポート作成機能を提供し、既存の運用、セキュリティ情報、イベント管理、セキュリティ･オペレーション・センタのワークフローを補完します。

ビジネス上の課題

あらゆる規模の企業に対して攻撃が増えています。さらに悪いことに、これらの攻撃は数週間、あるいは数か月も検出されず、企業の財政や評判に大きな被害をもたらします。そのため、特権アカウントを保護することが不正を防止し、コンプライアンスの要件に対応する上で不可欠です。しかし、従来の本人認証や権限認証のソリューションなどの静的制御では、今日の外部の攻撃者や悪意のある内部者による巧妙な攻撃を阻止することはできません。

現在の攻撃の防御を成功させるには、動的であることが重要です。それによって特権ユーザの動作が継続的に分析され、疑わしいアクティビティの特定、リスク分析、および攻撃されたアカウントや悪意のある内部関係者のアクティビティなどの問題の迅速な検出が可能になります。また、リスクの高いアクティビティや攻撃が検出された場合、1 つ以上の緩和策を自動的にトリガして、攻撃を阻止する必要があります。特権ユーザ動作分析と自動緩和策を統合してこれらが実現すれば、企業は外部の攻撃を阻止すると同時に、特権アカウントも保護できます。

ソリューションの概要

CA Threat Analytics for PAM を使用すると、外部ハッカーと内部脅威の両方を検出して停止するユーザ動作分析を展開できます。このソリューションの高度なアルゴリズムによって、特権ユーザの動作が継続的に分析され、履歴の所見や他のユーザの動作と比較されます。その結果、価値の高いアセットを調べたり、機密性の高いサーバからのデータ流出を試みたりするなど、攻撃や高リスクのユーザの活動が正確に識別されます。

アラートのみのソリューションとは異なり、CA Threat Analytics for PAM では自動的に制御機能をトリガして攻撃が阻止されるため、被害が制限され、検出されたリスクが緩和されます。たとえば、自動で追加の認証を生成したり、ユーザの不審なセッションを自動的に記録したりすることができます。

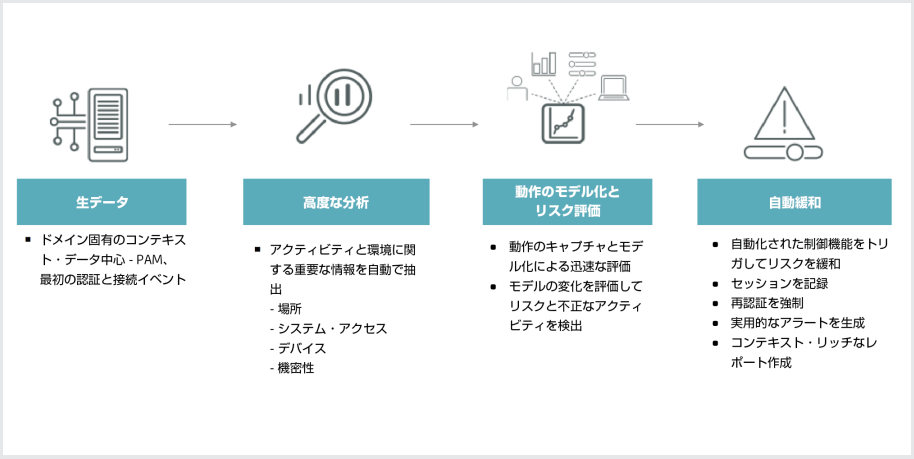
さらに、このソリューションは展開が容易で、インストール、設定、操作に特別なスキルを必要としません。

主な差別化要因

CA Threat Analytics for PAM では不正や内部関係者の誤用に対して、競合するソリューションを上回る強力な保護が提供されます。CA PAM ソフトウェアから収集したドメイン固有のコンテキスト・データに対して高度な分析が行われ、過去の動作パターンに基づいて作成されたリスク・モデルを使用してインテリジェントなリスクベースの判断が行われ、場合によっては緩和策が自動で即座にトリガされます。これらの機能では、以下が可能になります。

- **高度な分析：**各ユーザのアクションが詳細に分析され、ユーザの過去の動作モデルに基づいて評価されます。
- **PAM 固有の分析と機能：**特権アクセスを保護するために特別に構築されているため、一般的な分析ツール・キットのように統合、展開、微調整に多くの時間と労力をかける必要はありません。
- **自動緩和：**攻撃による被害を防止および制限する制御機能がすぐにトリガされるため、検出されたリスクを緩和します。
- **コンテキスト・リッチな表示とレポート作成：**強力なレポート・ツールにより、管理者はインシデントの調査、情報照会への対応、特権アカウントへのアクセス方法を簡単に理解できます。

CA Threat Analytics for PAM



関連製品

- **CA Privileged Access Manager** は物理、仮想化およびクラウドの環境で容易に展開できる特権アクセス管理の実績ある自動化ソリューションです。
- **CA Privileged Access Manager Server Control** では、オペレーティング・システム・レベルとアプリケーション・レベルのアクセスに対する詳細な制御機能によって、重要なビジネス・アセットを保護できます。
- **CA Identity Suite** では、オンプレミスおよびクラウド環境のすべてのユーザ・アクセスの管理および統制に使いやすいビジネス指向のユーザ・エクスペリエンスが提供されます。

サポートする環境

CA Threat Analytics for PAM は仮想アプライアンスとして展開でき、CA PAM バージョン v2.8 以降に対応しています。

詳細については、**ca.com/jp/PAM** をご覧ください。

CA Technologies（NASDAQ:CA）は、企業の変革を推進するソフトウェアを作成し、アプリケーション・エコノミーにおいて企業がビジネス・チャンスを獲得できるよう支援します。ソフトウェアはあらゆる業界であらゆるビジネスの中核を担っています。プランニングから開発、管理、セキュリティまで、CA は世界中の企業と協力し、モバイル、プライベート・クラウドやパブリック・クラウド、分散環境、メインフレーム環境にわたって、人々の生活やビジネス、コミュニケーションの方法に変化をもたらしています。詳細については **ca.com/jp** をご覧ください。