WHITE PAPER | 2017 年 3 月

企業のデータ・セキュリティ ユーザ動作分析の基本

ca technologies

目次

概要

現在、サイバー攻撃はメディアの見出しを独占しています。JP Morgan、Anthem、Slack の大規模な侵害など、注目を集めた攻撃は被害を受けた組織の外部からの攻撃ですが、特権ユーザによるデータの窃盗や誤用も増加しています。

実際、企業のセキュリティ専門家の 69%が、信頼できる内部関係者の手による企業情報の盗難や破損を経験したと回答しています [1]。また、サードパーティの契約業者、ベンダー、またはパートナーの故意または過失によってネットワークが侵害されることもあります。

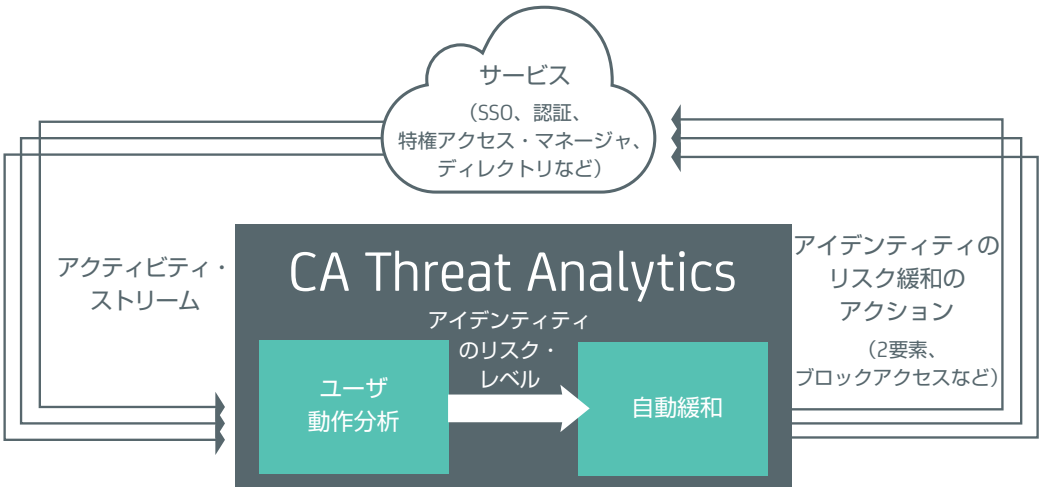
このような事実から、特権アクセスを保護することは、あらゆる規模の企業にとって緊急課題であることがわかります。しかし、セキュリティに対する意識が高まり、セキュリティ製品も過剰なまでに提供されているにもかかわらず、多くの IT システムは依然として攻撃に対して脆弱です。

実際、伝統的なアイデンティティ / アクセス管理（IAM）の制御は広範ではあるものの静的です。悪意のあるユーザがアクセスを取得したら、アカウントに設定された特権の範囲内でシステムを悪用することができます。

しかし、ユーザ動作分析や異常検出を自己学習モデルに統合するアイデンティティ中心のアプローチをセキュリティに導入すると、企業は危険なアクティビティを迅速に検出し、緩和策を自動的にトリガして被害を抑制できます。

CA Threat Analytics

CA Threat Analytics では、クレジット・カードによる金銭の保護と同じ方法で企業のデータが保護されます。これは、継続的に監視して、分析に基づいてリスクを判断し、「悪者」から資産の盗難を防止するということですが、これだけでは、具体的な方法はわかりません。このホワイト・ペーパーでは、CA Threat Analytics のユーザ動作分析と自動緩和という 2 つの関連する機能を使用して、企業のデータを保護する仕組みについて説明します。



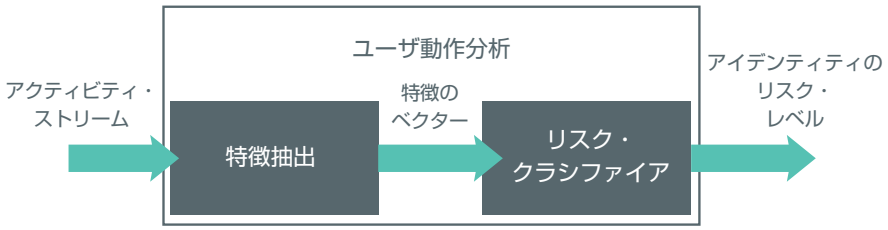
ユーザ動作分析では、リスクを継続的に評価して、不正なアクティビティを迅速に検出できます。ユーザ動作分析では、特定のアイデンティティやアイデンティティのグループとサービスやアプリケーションの間を行き来するデータ・ストリームを入力として取得し、各エンタープライズ・アイデンティティに関連するリスク・レベルを出力します。

自動緩和では、リスク緩和の手順と検出された不正なアクティビティを阻止する手順が自動的に実行されます。また、ユーザ動作分析のリスクの出力に基づいて、個々のアイデンティティに対するアクセスの制御方法が変更されます。自動緩和のわかりやすい例としては、特に機密性の高いアプリケーションまたはデータ・リポジトリへのリスクの高いアイデンティティのアクセスを自動的にブロックすることなどがあります。

ユーザ動作分析と自動緩和はいずれも CA Threat Analytics の機能に統合されていますが、このホワイト・ペーパーではユーザ動作分析に重点を置いています。以下のセクションではまず、先の図で示したユーザ動作分析の機能を構成要素に分解します。次に、各構成要素について詳しく説明します。わかりやすくするために、単一のサービスにおける単一のアイデンティティの保護を中心に説明します。手法の基本的な説明の後、複数のサービスに使用されるアイデンティティのグループを扱うときに、これらのアイデアがどのように強化されるかについて説明します。

基本

概念的には、ユーザ動作分析機能は、特徴抽出とリスク･クラシファイアという 2 つの要素で構成されています。



特徴抽出コンポーネントでは、アクティビティ・ストリームが処理され、必要な特徴が抽出されます。
必要な特徴とは、長期間に観察された個々のアイデンティティに関する以下のような特徴です。

- そのアイデンティティは未知のモバイル・デバイスを使用している。
- そのアイデンティティは遠隔地で操作されている。
- そのアイデンティティは不審な IP アドレスからアクセスしている。
- そのアイデンティティは特権グループのメンバである。
- そのアイデンティティはサービス X を通常の営業時間外に利用した。

特徴抽出は、現在のトランザクションに関する特徴を抽出するだけではないため、見た目よりも複雑です。アクティビティ・ストリームは一連の別々のイベントとして到達しますが、実際の入力は最初から完全なアクティビティ・ストリームです。そのため、各アイデンティティの使用と動作を総合的に把握できます。アクティビティの完全な履歴を確認できない場合、イベントごとに個別にリスクを評価しなければなりません。

たとえば、先に示した特徴の場合、単一イベントのコンテキストで通常の営業時間とはどのような意味であるかなどです。このような重要な特徴を CA Threat Analytics で使用するには、履歴データに関する計算と洞察も使用する必要があります。

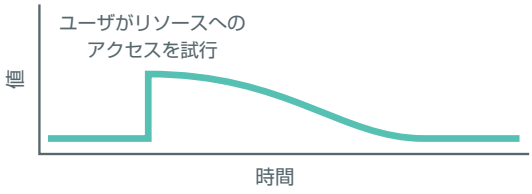
CA Threat Analytics では、完全なアクティビティ・ストリームが確認されるため、これまでのリスク評価や不正なアクティビティの検出よりもはるかに多くの洞察が提供されます。現在では、過去のアクティビティや個々のアイデンティティに関する特定の情報に基づいてリスクを評価できるようになりました。ただし、そのためには大量のデータを処理する必要があり、その大半が冗長なためにコストがかかります。幸いなことに、特徴抽出を実行すれば、データの次元が減少します。これにより、冗長なデータが排除または集約されるだけでなく、ユーザ動作分析機能の 2 つ目の要素であるリスク・クラシファイアに必要な情報が強調されます。

時間のコンテキストにおける値の判断

次に進む前に、観察する特徴について、興味深い点を取り上げて説明します。特徴はアクティビティが到達したときに変更されるため、専門的には時間領域に分類されます。簡単に言うと、値は時間の経過と共に変化するということです。特徴が観察されると、CA Threat Analytics ではその観察が時間の関数としてモデル化されます。つまり、アクティビティが到達して特徴が有効になると、その特徴の「値」は、そのアクティビティの時間で最大になり、時間が進むにつれて変化します。

実際の値の変化は、抽出された特徴によって大きく異なります。たとえば、値が 2 つしかない場合、特徴が観察されると、以下のように、その特徴が緩和されるまで最大値のままになります。

次に、機密グループのメンバを例に説明しましょう。その特徴は、アイデンティティがグループに関連付けられている全期間にわたって値が割り当てられます。その他にも、減衰パルスとしてモデル化される特徴があります。このタイプの特徴は、以下に示すように、観察されたときに最高値となり、時間と共に減衰します。



たとえば、ユーザが許可されていないリソースへのアクセスを試行した場合などです。この特徴は、その日のアイデンティティのリスク・レベルには関連しますが、1 週後には関連性が大幅に低くなり、1 か月後にさらに低くなります。特徴の値を時間の経過と共に減衰させることで、CA Threat Analytics では、その特徴が最も適切な方法でリスクに関連付けられます。

リスク・クラシファイア

リスク・クラシファイアは、特徴のベクターを 3 つの異なるリスク・レベルに変換する分析の関数です。

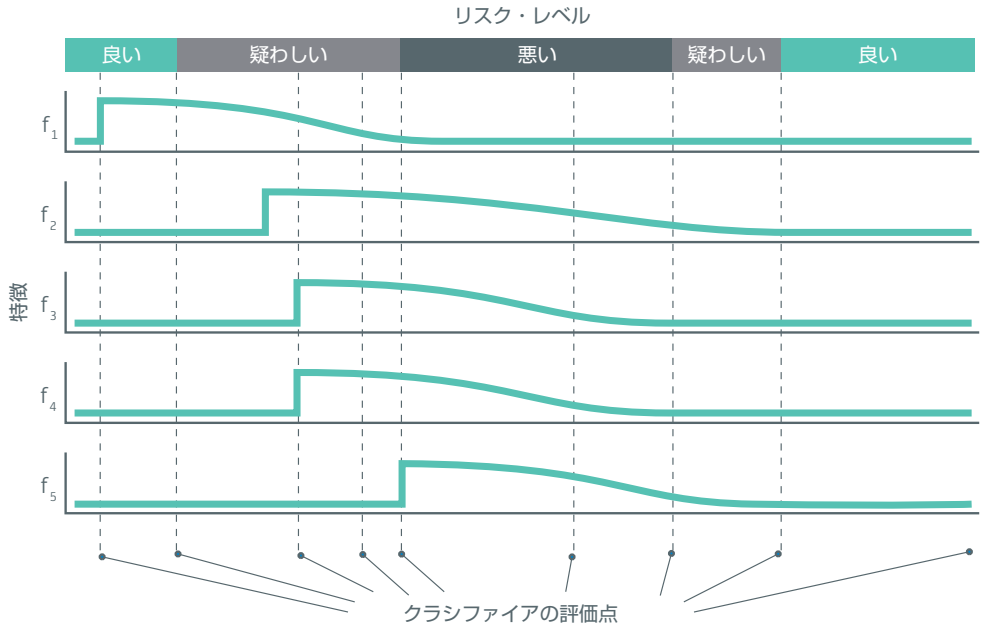
- **良い** - そのアイデンティティのリスクは最小限です。
- **疑わしい** - そのアイデンティティは、リスクを引き起こすイベントまたはアクティビティに関連していますが、即時のアクションを必要としません。システムはそのアイデンティティをより詳細に監視し、企業のポリシーに応じて最初の自動緩和策を実行できます。
- **悪い** - そのアイデンティティは高リスクとみなされ、即時の注意が必要です。企業のポリシーに従って、自動緩和とアラートが実行されます。

リスク・クラシファイアの関数によって、入力として特徴の値のベクターが使用され、上記の異なるクラスの 1 つが出力されます。

$$\text{クラシファイア}\ (\text{特徴}\ (t)) \longmapsto \{\text{良い、疑わしい、悪い}\}$$

前述のように、特徴自体は時間の関数なので、リスク･クラシファイアの関数も時間領域で使用されます。リスク･クラシファイアは一般的に、特徴のベクターの値の著しい変化に対応して、重要な判断を行うときに呼び出されます。特定の時点に対して、リスク・クラシファイアによってリスク・レベルが計算されるときは必ず、その時点におけるそのアイデンティティまたはエンティティのすべての特徴の関数も評価されます。リスク・クラシファイアが使用する実際の特徴のベクターは、その時点でエンティティに対して有効なすべての特徴によって構成され、リスクを判断するために使用されます。

下の図では、リスク・クラシファイアが評価する異なる時点の例を示しています。前述のように、特徴の値が増加したとき、および特徴の値がしきい値を下回ったときに評価が行われています。リスク・クラシファイアに渡される値は、評価がトリガされた時点の各特徴の値に相当します（上記の垂直の線が該当します）。もちろん、リスク・クラシファイアを実行するたびに新しいリスク・レベルになるわけではありません。実際には、特徴の値、システムのアクティビティ、脅威情報の変化に対応して、この図に示すより多くの評価点があります。一般にリスク･クラシファイアは、リスク・レベルの変化の可能性があるときに有効になります。



では、リスク・クラシファイアとは何なのでしょうか。どのようにして、特徴のベクターを異なるリスク・クラスの 1 つに変換するのでしょうか。これは、リスク・クラシファイアと対極にあるアプローチを説明した方がわかりやすいでしょう。CA Threat Analytics のリスク・クラシファイアは、「特徴 X が有効な場合は「悪い」を返す」というような、特定の特徴をテストする単純なルールではありません。この単純なアプローチは、従来の多くのセキュリティ製品で使用されています。しかし、このアプローチでは誤検出が発生しやすく、脆弱で簡単に攻撃されてしまうため、見事に失敗します。さらに、このアプローチでは、不正なアクティビティの検出と正規ユーザによるシステムの使用の両方に必要な情報が使用されません。

CA Threat Analytics は、このようなアプローチよりもはるかに強力です。CA Threat Analytics のリスク・クラシファイアは、単独ではなく、一連の特徴全体のコンテキストで特徴を検査します。このアプローチでは、孤立してリスク・レベルに影響を与えない特徴を組み合わせて、意味のある方法でリスクに反映することができます。さらに、CA Threat Analytics には、個々のユーザやアイデンティティの集合体の変化の状況を含め、デプロイされたシステムからのフィードバックが組み込まれているため、時間の経過と共に判断が向上します。その結果、新しい脅威やデプロイ・シナリオにも柔軟に対応できるシステムが実現します。

集合体とサービス

前述のように、これまでの説明はわかりやすくするために簡略化されています。まず、アイデンティティの集合体はどうなるのでしょうか。特に企業環境には、特定のアイデンティティのリスク・レベルに関連するさまざまなアイデンティティのグループがあります。たとえば、以下のような場合です。

- 通常よりも多くのデバイスでリソースにアクセスする
- グループが通常操作する場所以外で操作している
- 不当に多数のグループに属している

ユーザに関連付けられている通常のデバイス数、組織における操作の場所、グループの適切な数などの要因を含め、期待されるアクティビティのベースラインは組織によって異なります。単独のアイデンティティではなく、アイデンティティのグループを使用すると、有用性に優れた集合体の統計が得られ、個々のアイデンティティの比較に使用できます。もちろん、それにはコストがかかります。そのため、単にアイデンティティのアクティビティ・ストリーム全体を処理だけでなく、組織全体のアクティビティの完全な履歴から特徴を抽出します。

同様に、単一のサービスからサービスのグループに分析を拡大することで、異なる利点がもたらされます。複数のサービスにおけるアイデンティティのアクションを調査すると、特徴を抽出して一般的なアクセス・パターンのモデルを構築し、それらをインテリジェントに適用してすべてのサービスにセキュリティを提供できます。また、その情報を使用して、CA Threat Analytics では、そのアイデンティティまたは企業にとって脅威となる異常で一貫性のない動作を検出できます。

まとめ

このホワイト・ペーパーでは、CA Threat Analytics でユーザ動作分析を使用して、企業のデータを保護する方法を紹介しました。基本的なアイデアは簡単に説明できますが、特徴抽出とリスク・クラシファイアの具体的な問題はこの文書では説明しきれません。実際、リアルタイムの意思決定を可能にし、長期的にシステムの正確性を確保し、システム管理者にリスクを判断するための完璧な洞察を提供するなど、実際の要件の多くについては言及していません。

これらの要件の詳細、およびそれらを組織で活用する方法については、以下をご覧ください。https://www.ca.com/us/products/ca-threat-analytics-for-privileged-access-manager.html

ca.com/jp/でCA Technologiesにアクセスしてください

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。

1 Accenture および HfS Research「The State of Cyber Security and Digital Trust 2016」2016 年 6 月：https://www.accenture.com/t20160704T014005__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf#zoom=50

CS200-259092