RSA

RSA NETWITNESS® UEBAのユースケース

ユーザーベースの脅威に対する強力な検出機能

RSA NetWitness UEBAは、RSA NetWitness Platformの中心的な要素として組み込まれた、ユーザーおよびエンティティ振る舞い分析専用のBig Data駆動型ソリューションです。RSA NetWitness UEBAは、教師なし統計的異常検出と機械学習を活用することで、未知の脅威を行動ベースで包括的に検出し、幅広いユースケースに対応します。RSA NetWitness UEBAは、既存のセキュリティ チームを強化して、攻撃ライフサイクルのすべてのステップで迅速な検出と実践的なインサイトを提供します。

ユーザーおよびエンティティ振る舞い分析（UEBA）ソリューションを評価するときは、次の重要な機能が備わっているかどうかを調べます。

- 完全に自動化された継続的な脅威の検出と監視
- データの収集、検出、調査、対応を活用した攻撃ライフサイクル全体の可視性
- MITRE ATT&CK™フレームワークと連携する自然言語インジケーター
- チューニング不要でゼロタッチのターンキー データ サイエンス モデルによる教師なし機械学習
- プラットフォームの中核であり、ログ収集とエンドポイントでの検出および応答を組み合わせたエンドポイント エージェント

エンタープライズ クラスUEBAのコア機能

ネイティブのデータ収集

多くのSOCチームにとって重要な課題は、自社のオンプレミス システムとクラウドベース システムの膨大なポートフォリオによって生成される、さまざまな形式のログの収集、保存、分析を管理することです。RSA NetWitness UEBAは、これらのシステムからrawログデータを収集し、人とプロセスによって生成されたさまざまなソースからのアクティビティを動的に解析して、これらのデータ ソースからの重要なセキュリティ情報を解釈することによって、この課題に対処します。

統合メタデータの分類

UEBAソリューションを最適に実行するには、ログ、ネットワーク トラフィック、エンドポイント データのフィードを解析し、取得時に正規化して、一貫性のある統合メタデータ分類に変換する必要があります。RSA NetWitness UEBAは、RSA NetWitness Platformの全方位型SIEMの中心的なコンポーネントであるため、これは自動的に行われます。

機械学習のスピードで検出

ほとんどの場合、ポイント セキュリティ ソリューションからの脅威の痕跡や証拠は、攻撃を識別する信頼性と一貫性のある方法ではありません。なぜならば、これらのアクティビティは単独では攻撃の一部ではなく、そのたびにアラートを発行していると、アナリストが膨大な量のアラートに埋もれてすぐに行き詰ってしまうからです。RSA NetWitness UEBAは、アクティビティと動作のパターンを一定期間にわたって確認し、機械学習を使用してベースライン動作の偏差を識別し、誤検出としてマークされた過去のアラートから学習するため、ポイント セキュリティ ソリューションよりもフォーカスを絞った実践的なアラートを生成できます。

UEBAが中心的なセキュリティ要件になった理由

- 報告された侵害の28%は内部の攻撃者に起因しています。UEBAは、これらの種類の脅威の検出を容易にします
- 報告された侵害の原因となっている最多の内部関係者は、システム管理者とエンドユーザーです
- 侵害の68%は、発見するのに2か月以上かかりました。UEBAは、セキュリティ チームが脅威をより迅速に検出するのに役立ちます
- 報告された侵害行為の最たるものは、認証情報の盗難と特権の乱用/誤用です。UEBAはこれらのアクティビティについて警告するよう設計されています

Verizonの『Verizon Data Breach Investigations Report 2018』

詳細はこちら

RSA.com/DoMoreをご覧になるか、デモをご予約ください

RSA

RSA NETWITNESS UEBAが検出するよう設計されている6つのユースケース

異常なアクション/変更

攻撃者がActive Directory（AD）ドメインまたはドメイン コントローラーへの特権アクセスを取得した場合、攻撃者はそのアクセス権を使用してADフォレスト全体を制御または破壊することができます。ドメイン コントローラーのうち1つでも侵害されれば、そのコントローラーに対する変更が他のすべてのシステムに複製される可能性があります。RSA NetWitness UEBAは、アカウントが侵害されている可能性、または重要なディレクトリー データを破損または破壊するために使用されている可能性を示しているADドメインに対するユーザー アクションの急増を特定して、アナリストがこれらのタイプのシナリオを検出するのを支援します。

異常な特権ユーザー アクセス

RSA NetWitness UEBAを使用して、特権ユーザーが内部関係者による脅威をもたらす可能性がある場合にそれを特定できます。たとえば、ヘルプデスクの技術者が「通常の」ルーチンと確立されたセキュリティ ポリシーから逸脱し始め、新しいユーザーのパスワードの有効期限を無期限に設定し始めた場合は、RSA NetWitness UEBAでそれを検出できます。

スヌーピング

スヌーピングとは、他人または会社のデータへの不正アクセスを指します。通常は、価値の高い企業情報を見つけて取得するために、自分がアクセス権を与えられていないサーバーやフォルダーを参照しようとする内部のユーザーまたは外部の攻撃者によって行われます。高度なスヌーピングでは、パソコン上のアクティビティをリモートで監視したり、自動ファイル検出を実行したりするカスタム プログラムが利用されます。

RSA NetWitness UEBAは、さまざまな方法でスヌーピングを検出できます。ユーザーが正当なアクセス権を持たないデータにアクセスしようとした場合に、アクセスの失敗回数と成功回数を取得します。新しい場所への成功および失敗ファイル アクセス試行が短時間で異常に多く行われていることを特定した場合は、アラートをトリガーします。

ブルートフォース認証

高度なUEBAソリューションは、失敗した認証を異常なユーザー アクティビティに照らして検証することで、真のブルート フォース攻撃と悪質ではない認証失敗を区別できます。RSA NetWitness UEBAは、認証の失敗の繰り返しに加えて、不審な行動パターンを検出した場合にのみアラートをトリガーします。これにより、ネットワーク設定の不備に関連した誤検出や、パスワードを思い出せないユーザーに関連した誤検出を排除できます。

マシン主導のアクティビティ

RSA NetWitness UEBAでは、悪意のあるプログラムが侵害された認証情報を使用して、アクセス制限された企業リソースにアクセスしようとしていることを検出できます。ユーザー プロファイリングはブルート フォース攻撃の兆候を明らかにし、エンティティ プロファイリングは不審なエンティティの振る舞いの急増を特定できる可能性があります。これには、数百個のアカウントに対する過剰な数のアクティビティが単一のデバイスまたはIPアドレスから行われている場合や、複数のマシンにわたって大量のファイル名変更が行われ、それらすべてが悪質なプログラムがインストールされている単一のマシンから行われている場合が当てはまります。

権限の昇格

攻撃者は、往々にして標的にしやすい組織の正規のユーザーを利用して、昇格された特権を自分自身に付与することによって、さらなるネットワーク攻撃を仕掛けようとします。特権ユーザーのアクティビティ、付与されたアクセス権、機密グループなどを注意深く監視することは、認証情報の侵害に対抗する上で重要です。ただし、特権ユーザーが常に「通常の」行動パターンに従うとは限らないため、誤検出は避けられません。したがって、悪意のある痕跡を特定するには、痕跡の蓄積を識別、収集、解析することが重要です。

認証の試行が複数回失敗した後で、通常とは異なる場所からログオンした攻撃者が特権を昇格した場合、その特権を使って新しいユーザー アカウントが作成されると、最重要アラート リスト内の高リスクとして報告されます。

セキュリティ スタックに別のポイント ソリューション（この場合はUEBA）を追加する前に、それによって真に付加価値がもたらされるのか、それとも単に負担が増えtるだけなのかをよく考えてください。RSA NetWitness UEBAのメリットは、従来の脅威に加え、ユーザーベースの重大な異常も単一のプラットフォーム内で検出できることです。