# RSA NETWITNESS® UEBA

### 主な特長:

- *特許取得済みで再帰型の教師なし振る舞い機械学習*
- *ネイティブのデータ収集*
- *革新的な機能の重み付けシステム*
- *シンプルになったリスクスコア付けエンジン*
- *幅広いユースケース*
- *アイデンティティー コンテキストの可視化*
- *自動化された誤検出削減アルゴリズム*

### 主なメリット：

- *MTTDとMTTIの短縮*
- *インシデント対応の迅速化*
- *誤検出の減少*
- *アイデンティティーベースのコンテキスト エンリッチメント*
- *リスクの高いユーザーを迅速に特定*

*進化する破壊的な脅威がどこで生じているかにかかわらず、効果的に対抗できます。*

## 脅威の迅速な検出、滞留時間の短縮、対応の自動化

攻撃対象領域が拡大し続ける時代に、コモディティ マルウェアから内部関係者による脅威、クライムウェア、国家主導によるエクスプロイトに至るまで、脅威アクターからデータや資産を保護することは、ますます複雑な作業になっています。すべての脅威が同じように発生するわけではありません。しかし、予防、監視、調査のためのテクノロジーが分断された状態では、セキュリティ オペレーションセンター（SOC）は誤検出を迅速に排除できず、互いにつながりのないアラートを無数に送るだけで、フォーカスを絞ったインジケーターを提供することはできません。必要なのは、組織にとって最も重要な脅威をセキュリティ アナリストが検出して対応できるようにする、包括的で協調的なソリューションです。

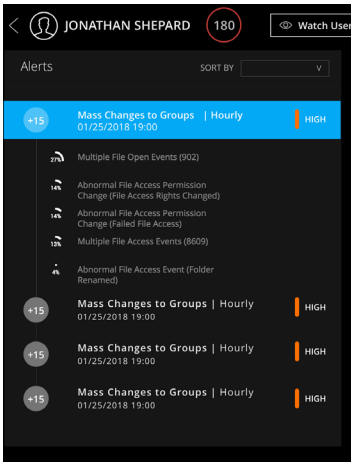
RSA NetWitness® UEBAは、RSA NetWitness Platformの中心的な要素として組み込まれた、**ユーザーおよびエンティティ振る舞い分析**専用のBig Data駆動型ソリューションです。RSA NetWitness UEBAは、教師なしの機械学習アルゴリズムを幅広いユースケースにわたって活用することで、アナリストによる調整を必要とせずに、振る舞いに基づいて未知の脅威を包括的に検出できます。RSA NetWitness UEBAは、既存のセキュリティ チームを強化して、攻撃ライフサイクルのすべてのステップで迅速な検出と実践的なインサイトを提供します。RSA NetWitness UEBAは、RSA NetWitness Platformの中核であり、攻撃調査のライフサイクル全体を対象に侵害解決を支援します。

## あらゆる環境で脅威を検出

RSA NetWitness UEBAは、RSA NetWitness Platformの自動化された脅威検出機能を強化します。セキュリティ アナリストは、RSA NetWitness Platformにネイティブで備わったコア機能のネットワーク キャプチャ、ログ収集、エンドポイント可視性、機械学習のスピードでの統合メタデータ エンリッチメントを活用して、明確でフォーカスを絞ったアラートを通じて、内部と外部の両方の攻撃者を排除できます。RSA NetWitness UEBAは、人工知能と優れた機械学習の数学的アプローチを利用して、ユーザーとユーザー グループ、エンティティ、および組織全体の振る舞いのベースラインを設定することで、悪意のある逸脱から悪意のない正常な活動を分離して、真に実践的なインシデント対応を実現します。

## 終わりのない質問ではなく、明確な答えを提示

RSA NetWitness UEBAは、MITRE ATT&CK™フレームワークと連携して不審な痕跡情報を指摘し、セキュリティ アナリストがアイデンティティーベースの時系列の可視化によって侵害のソースや不審で異常なアクティビティのソースを特定できるようにして、より効率的で完全なインシデント対応を実現します。



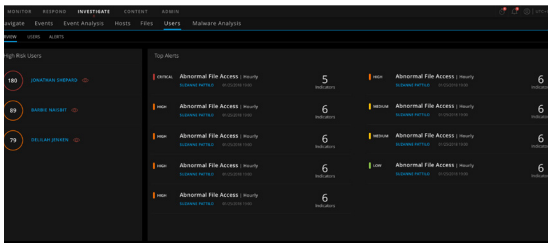
RSA

## UEBAのユースケース：

- *内部関係者による脅威*
- *総当たり*
- *アカウントの乗っ取り*
- *侵害されたアカウント*
- *特権アカウントの悪用と誤用*
- *権限の昇格*
- *ユーザーのスヌーピング*
- *データの窃取*
- *異常なシステム アクセス*
- *横方向の移動*
- *悪意のあるアクティビティ*
- *不審な振る舞い*

*RSA NetWitness UEBAは導入した瞬間にスマートに動作して、異常な振る舞いを迅速かつ正確に明らかにし、ユーザーが絶えず調整を加える必要はありません。*

## 介入不要の検出機能



自動化された継続的な監視により、ルール、シグネチャ、または手動による分析なしで、侵害されたアカウントを使用している不正な内部関係者とサイバー犯罪者の両方を迅速に検出できます。RSA NetWitness UEBAは、強力なデータ サイエンス モデルによって、未確認のツール、テクニック、プロセス（TTP）を検出する組織の能力を強化するとともに、エンドツーエンドの調査機能を提供して、アナリストが組織全体のリスク状況を未加工の分析結果から把握できるようにします。

Big Dataのスケーラブルなテクノロジー アーキテクチャを活用するRSA NetWitness UEBAには、強力な脅威検出エンジンが備わっており、バラバラなイベントをつなげて、異常なアクティビティやこれまで未知だったユーザーの脅威をすべて単一のユーザー インターフェイスで表示することが可能です。

## UEBA、プラットフォームの中核

明確で実践的、かつコンテキスト認識型のアラートにより、不審なアクティビティを示している可能性の高いユーザーの行動に的を絞り、最終的にはセキュリティ アナリストの対応を強化できます。RSA NetWitness Platformは、進化する脅威と同じ俊敏性とスピードで動作できる、適応型のユーザーおよびエンティティ振る舞い分析を導入します。RSA NetWitness Platformは、動的で非決定的な検出アルゴリズム、ベースライン設定、動作モデリング、ピアグループ分析を活用して、自動化されたログ データを取得して、セキュリティ アナリストが攻撃者の正体を暴けるようにします。

RSA NetWitness UEBAとUEBA Essentialsは、ログ イベント、ネットワーク トラフィック、エンドポイントの可視化によってリアルタイムで相関付けられた、優先度の高いイベントを明らかにすることで、SOCチームがMTTD（平均検出時間）とMTTI（平均調査時間）を短縮し、アラート疲労と誤検出を軽減できるようにするほか、より正確な脅威予測と予測分析を効果的に提供できるようにします。

## RSA NETWITNESS PLATFORM

30年以上のセキュリティ専門知識を持つRSAは、世界中のセキュリティ オペレーション組織の課題に対処できる、革新的なソリューションで市場をリードし続けています。新しいRSA NetWitness UEBA製品は、ログ、ネットワーク、およびエンドポイント全体にわたる広範な可視性を活用して、RSA NetWitness Platformとその全方位型SIEMと脅威防御製品を拡張します。

最新の統合、導入事例、ベスト プラクティスについては、RSAのWebサイト（RSA.com/DoMore）をご覧ください。