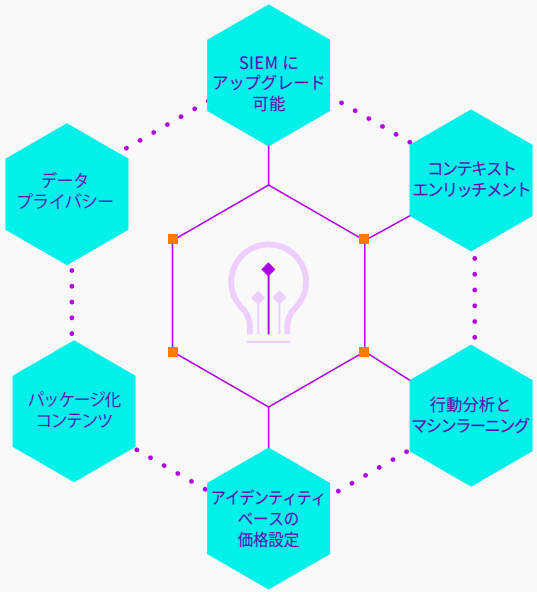
securonix

データシート

User and Entity Behavior Analytics

環境内に隠れた脅威の検知と調査



未知の脅威とインサイダー脅威の検知

サイバー攻撃が巧妙になるにつれ、これらの脅威を検知することは難しくなります。従来方式のルールベースのアプローチでは、フォールスポジティブのアラートが大量に発生するため、高度な脅威に対しては効果がありません。

Securonix UEBA は、クラウド上でもオンプレミスでも、組織内の異常なユーザー行動、不審なラテラルムーブメント、インサイダー脅威を検知します。組み込み API を使用して、クラウド環境のすべての主要なインフラストラクチャ、多くのセキュリティやビジネスアプリケーションに対する監視ができます。さらに、マシンラーニングと標準実装されたユースケースコンテンツを活用することで、ノイズを低減し、SOC チームは、最もリスクの高いアラートに集中できます。

高度な脅威やインサイダー脅威の先を行く

悪意か不注意かを問わず、インサイダー脅威は常にリスクです。従来方式のセキュリティソリューションでは、行動の変化を識別できないため、高度な脅威やインサイダー脅威を検知することはできません。そのため、被害があった後に対処するか、攻撃が行われたという事実に気づくことさえできません。

Securonix UEBA は、インサイダー脅威のリスクを低減するのに役立ちます。ユーザーとエンティティの行動を監視し、より積極的なアプローチを行います。マシンラーニングと分析を使用して、ユーザーの行動パターンにリスクスコアを割り当てます。高リスクのユーザーは、セキュリティチームが識別できるよう区別して表示され、アナリストは、ユーザーをウォッチリストに追加したり、そのユーザーの行動をさらに調査したりできます。Securonix UEBA は、データ窃取、特権アカウントの不正使用、侵害されたユーザーアカウント、ボットネット感染などの行動に関するアラートを発します。

行動分析による誤検知とノイズを低減

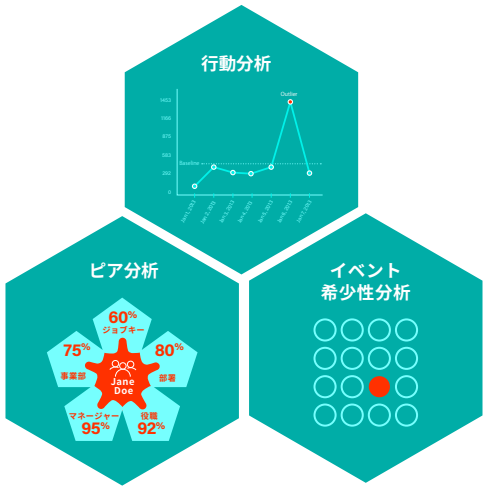
多くの SIEM ソリューションでは、膨大な量のフォールスポジティブのアラートが発生し、被害を止めるために、真の脅威をタイムリーに特定することが困難になります。Securonix UEBA を使用すると、複数イベントにまたがる脅威を関連付け、最小限のノイズで巧妙な脅威を発見できます。

脅威の検知を迅速化

コンテキストや関連イベントに結び付かない、単一のセキュリティアラートは、脅威を検知する方法としては有効なものではありません。脅威のキルチェーンにも適用できる Securonix の脅威モデルを使用すると、効率よく、より迅速に脅威を検知することができます。脅威モデルでは、関連する一連のイベントをつなぎ合わせます。アナリストは、脅威モデルによる単一のアラートによって、関連するすべてのイベント情報を得ることができ、複数の個別アラートをそれぞれ追跡する必要がありません。Securonix を使用すると、巧妙な脅威をより迅速に特定できます。

巧妙化した脅威やインサイダー脅威を高度な分析で検知

インサイダー脅威を検知するには、正常な行動と不審な行動を見分けることが極めて重要です。Securonix UEBA は、脅威チェーンと高度なマシンラーニングによる行動分析を使用して、巧妙な脅威やインサイダー脅威を検知します。



脅威チェーン：「ロー・アンド・スロー」アタックを特定するために、関連するイベントをつなぎあわせて、アラートの量を低減します。脅威モデルは、MITRE ATT&CK、US-CERT 、両方のフレームワークにマップされています。

行動分析：標準実装された分析コンテンツは、巧妙化した脅威を最小限のノイズで迅速に検知します。Securonix の特許取得済みのマシンラーニングアルゴリズムは、確立した行動ベースラインから逸脱した複数の脅威に関するアラートを上げます。

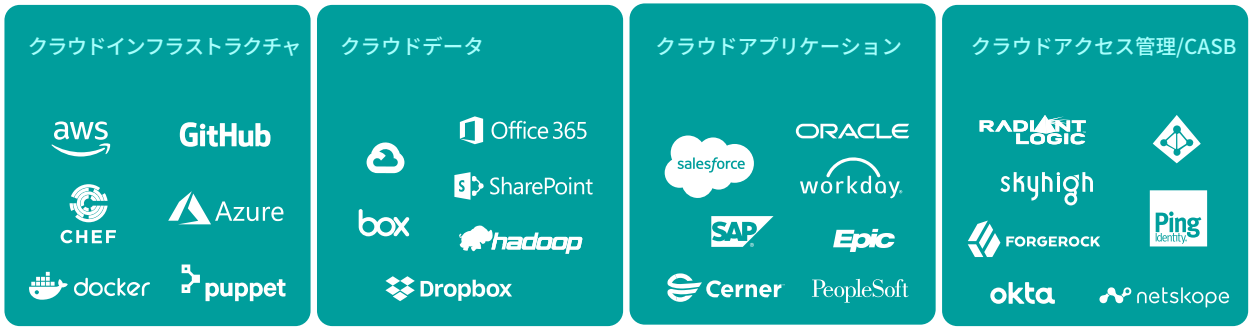
迅速な価値の実現

Securonix UEBA は、迅速に導入でき、検知と対応における迅速な価値の実現をする、Saas ソリューションです。すぐに使用できるコンテンツとして、脅威モデル、ユースケース、組み込みのコネクターが標準実装されているため、迅速に導入し、巧妙化した脅威を迅速に特定できます。

ユースケース：インサイダー脅威、IP 窃取、不正行為などに対応するコンテンツに、クリック 1 回でアクセスでき、即座に恩恵を受けることができます。

コネクター：コネクターを標準実装しているため、Securonix UI を使用して、迅速、正確、効率的に脅威の調査と対応ができます。100 を超える標準実装のクラウドコネクターにより、ハイブリッドインフラストラクチャ全体の、さまざまなソースからデータを取り込むことができ、組織内のリスクの全体像を把握できます。

クラウドコネクター



SIEM投資のROIを最大化

既存の SIEM を廃止または交換することなくアップグレードできます。Securonix ソリューションの柔軟なテクノロジースタックに基づき、UEBA 分析機能を追加することで、現在ご使用のレガシーソリューションを容易にアップグレードできます。

SIEM+UEBA: Securonix UEBA は、あらゆる SIEM とシームレスに統合できます。既存のソリューションを置き換えることなく、既存のセキュリティ投資へのコスト削減を実現できるよう支援します。

クラウドネイティブ：クラウド上に構築された Securonix のプラットフォームは、インフラストラクチャの管理が一切不要で、お客様の IT 環境にあるすべてのデータを活用できます。

Securonix UEBAの詳細については、
www.securonix.com/request-a-demo でお申し込みの上、デモをご覧下さい。

securonix