securonix

データシート

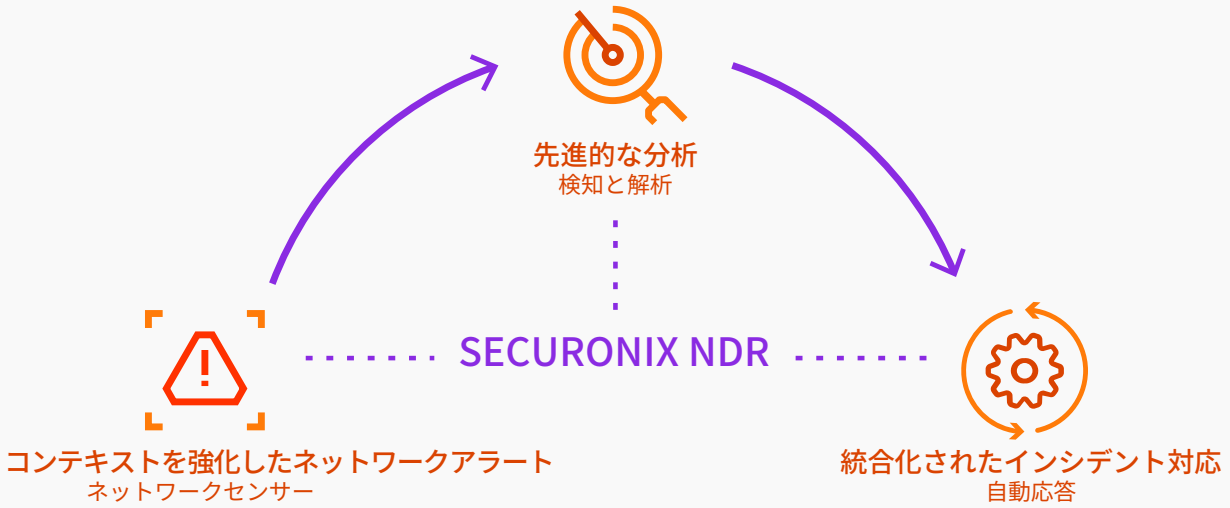
NDR (Network Detection and Response)

強力でスケーラブルなネットワークフォレンジック

Securonix の特性

ネットワーク攻撃による脅威は検知が難しく、従来のネットワーク保護ツールやファイアウォールでは、必ずしも全体像を把握できるとは限りません。Securonix Network Detection and Response (NDR) は、IT 環境全体のセキュリティインシデントとネットワークアクティビティの相関分析を行い、Next-Gen SIEM がその相関性を検知した場合、セキュリティチームに異常を警告することで、この課題を解決します。

Securonix NDR は、大きく充実したネットワークの可視性とコンテキスト等、すべてを単一のコンソールにまとめ、セキュリティチームが組織をサイバー脅威から保護できるよう支援します。



検知と対応にもたらすネットワーク可視化の真価

SIEM の投資効果を最大化

スタンドアロンの NDR や SIEM ソリューションでは検知できない高度な脅威を特定します。セキュリティチームは、ネットワークとセキュリティのすべてのデータが 1 か所に集約されることで、巧妙化した脅威を検知して対応するのに必要な、コンテキストを含む調査の手がかりを得ることができます。

ブラインドスポットに及ぶ可視化

NDR は、ネットワークアクティビティを他の IT 環境のデータと合わせて収集し、集約することによって、ブラインドスポットに対する可視化を実現します。Securonix Next-Gen SIEM と組み合わせることで、ネットワーク、エンドポイント、さらにそれら以外の範囲にまで及び、ユーザー、アカウント、システム行動を追跡しリアルタイムで脅威を検知して対応します。

巧妙化した脅威を検知

高度なサイバー攻撃は、多くの場合、ゆっくり時間をかけた複数のステップから成り、検知を困難にします。Securonix は、マシンラーニングと強力な分析を活用し、それらを異なる IOC から構成される脅威パターンとして検知をします。このソリューションは、SOC へのノイズを低減しながら、複数のアラートから構成される巧妙化した脅威を、対処すべきインシデントとして単一化します。

コネクテッドエコシステム

ネットワークセンサー：ネットワークデータを取り込み、セキュリティインテリジェンスを用いてエンリッチメントを行い、多様なネットワークセンサーからのデータを他のセキュリティデータと相関付け、SIEM にさらに深いインテリジェンスを提供します。Corelight、Verizon Protectwise、Gigamon との戦略的パートナーシップを含む、すべての主要なネットワークセンサー製品とのインテグレーションをサポートしています。

ネットワーク脅威ハンティング：ログ、エンドポイント、ネットワークデータを全方位の視点で可視化し、脅威ハンティングを支援します。対象をネットワーク脅威にまで拡大すると、より迅速に点を線として識別でき、検知と対応に要する時間を短縮できます。

Securonix NDR - 可視性、検知、先進的な分析

実効性のある分析

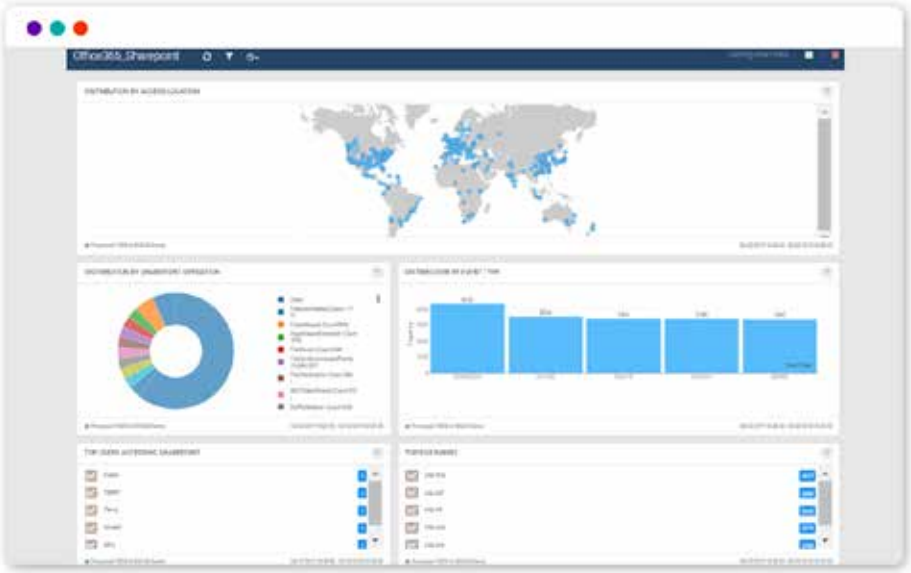
脅威チェーン：MITRE ATT&CK、US-CERT フレームワークに対応する脅威チェーンモデルを使用して、アラートの量を低減します。脅威チェーン分析は、アイデンティティコンテキストを使用して、ネットワークイベントとセキュリティイベントの両方にまたがる「ロー・アンド・スロー」アタックを追跡できます。

先進的な分析：マシンラーニングを活用した先進的な分析は、ネットワーク行動が、確立されたベースラインから逸脱していることを把握できます。これは、今日の複雑な環境において非常に重要であり、ルールベースのアプローチでは、大量の誤検知のアラートが出てしまいます。

全体データを把握

単一プラットフォーム：単一の完全に統合化されたバックエンドアーキテクチャにより、オペレーションの煩雑さを軽減します。セキュリティチームは、インフラストラクチャの管理が不要なため、脅威が次のステージに進む前に検知に専念することができます。

強力なレポート：ネットワークトラフィックに関するレポート、組み込みの共有可能なダッシュボードなど、包括的なネットワークデータを活用して、データに基づく意思決定ができます。統合プラットフォームは、セキュリティチームのコラボレーション、脅威ハンティングの最適化を支援します。



統合型されたインシデント対応

統合された SOAR は、インシデント対応に要する時間を短縮します。効率的な自動化を実現し、アナリストの対処を支援するプレイブックアクションが活用できます。

Securonix NDR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。