DATASHEET

WATCHGUARD THREATSYNC

XDRで脅威に対する早期の検知と迅速なレスポンスを実現

脅威のさらなる複雑化とセキュリティ技術の普及により、組織がセキュリティの情勢を包括的に把握し、対策することが難しくなっています。同時に、セキュリティチームは、高度な脅威に対して限られた可視性の中で、連携性に欠けるセキュリティツールを用いなければならず、脅威の検知にも時間がかかり、的確にレスポンスすることが困難な状況となっています。今日のセキュリティのエキスパートたちは、進化する脅威を特定し、封じ込め、迅速にレスポンスするための統合型セキュリティソリューションを必要としています。

ThreatSyncは、検知結果を一元化し、脅威に対して統合的にレスポンスするXDR機能を企業に提供します。サイバーセキュリティを簡素化しながら、可視性を向上させ、組織全体に渡るレスポンスアクションをより迅速に自動化し、リスクとコストを削減しつつ、より高い精度を実現します。

進化するサイバー脅威に対してプロアクティブに防御

可視性の拡大

ウォッチガードの最新テクノロジーによる緊密な連携とクロスドメインのデータテレメトリにより、優れたXDR戦略を構築することができます。増え続けるセキュリティスタックからのデータフィードの範囲を広げることで、可視性が大幅に向上し、より強力な保護体制を築くことが可能になります。

早期の検知

サイロ化されたセキュリティアプローチから脱却し、複数のソースからもたらされる脅威インテリジェンスによる検知が可能になります。ThreatSyncは、AIとML（機械学習）技術を用いて、複数のドメインにわたって潜在的な脅威をリアルタイムで特定し、平均検知時間（MTTD）を短縮します。

迅速なレスポンス

XDRを実行に移し、脅威に対して瞬時にレスポンスすることが可能になります。ThreatSyncにより、よりシンプルで迅速なプロセスで企業全体の脅威を無力化する自動レスポンスアクションを可能にすることで、平均レスポンス時間（MTTR）を短縮し、リスクを低減して高い精度を提供します。

ThreatSyncは、広く統一された可視性、統合的な検知、脅威への自動レスポンス、そして予算、規模、複雑さに関係なくあらゆる組織に適した機能により、セキュリティのエキスパートはセキュリティスタックをフルに活用することができます。

> ThreatSyncは、広く統一された可視性、統合的な検知、脅威への自動レスポンス、そして予算、規模、複雑さに関係なくあらゆる組織に適した機能により、セキュリティのエキスパートはセキュリティスタックをフルに活用することができます。

特長

優れた可視性

ネットワークおよびエンドポイントの活動を幅広く可視化し、検知されにくい脅威の特定を支援します

包括的なセキュリティ

シングルプラットフォームにデータやアラートを統合し、各セキュリティ機能が連携して脅威に対して優先付けし、レスポンスすることができます

セキュリティチームの負荷を削減

脅威の検知とレスポンスプロセスを自動化することで、セキュリティチームの時間とリソースを節約することができます

レスポンスプロセスを合理化

検知された脅威に対して、連携し、自動化されたレスポンスを実現します

XDRの追加コスト不要

XDR は現代のサイバーセキュリティに不可欠な要素であり、全ての企業が利用できるようにする必要があるため、ウォッチガードではThreatSyncを追加費用なしで提供しています

統合型のXDRベースのアプローチ

ThreatSyncは、ウォッチガードのUnified Security Platform（統合型セキュリティプラットフォーム）アーキテクチャの一部であり、セキュリティ環境を効果的に構築し、進化させるための基礎となるものです。また、組織のエコシステム全体におけるセキュリティの可視化を簡素化するように設計されています。これにより、セキュリティの専門家は、一連の連携した検知／レスポンス機能を装備することで、高度なサイバー脅威に対してよりプロアクティブに対応することができます。

脅威を統合的に可視化

ThreatSyncは、管理者が複数のコンソールを習得し、使用する必要がなく、コンピュータ、サーバ、ファイアウォールからの検知結果を単一のインターフェイスで収集し、表示します。これにより、管理者の管理負荷が減り、検知結果のコンテキストを把握し、高度な脅威を迅速に阻止してセキュリティリスクを低減することができます。

脅威を統合的に検知

ThreatSyncは、運用内容を自動的に相関分析し、各セキュリティレイヤの関連する活動と連携し、疑わしい活動を管理者に警告します。そして、侵害の指標（IoC）となり得る不正なシナリオをスコアリングして検知することで、平均検知時間（MTTD）の削減と影響、重大性、範囲の迅速な封じ込めを可能にします。

レスポンスを統合的に自動化

セキュリティのエキスパートたちは、必要な情報さえあれば、容易かつ迅速にレスポンスすることができます。ThreatSyncは、企業全体で一元的に脅威に対して迅速なレスポンスアクションをスケジューリングし、自動化し、あるいはオンデマンドで実行する機能を提供しており、ITおよびセキュリティチームはより効率的に作業することが可能になります。

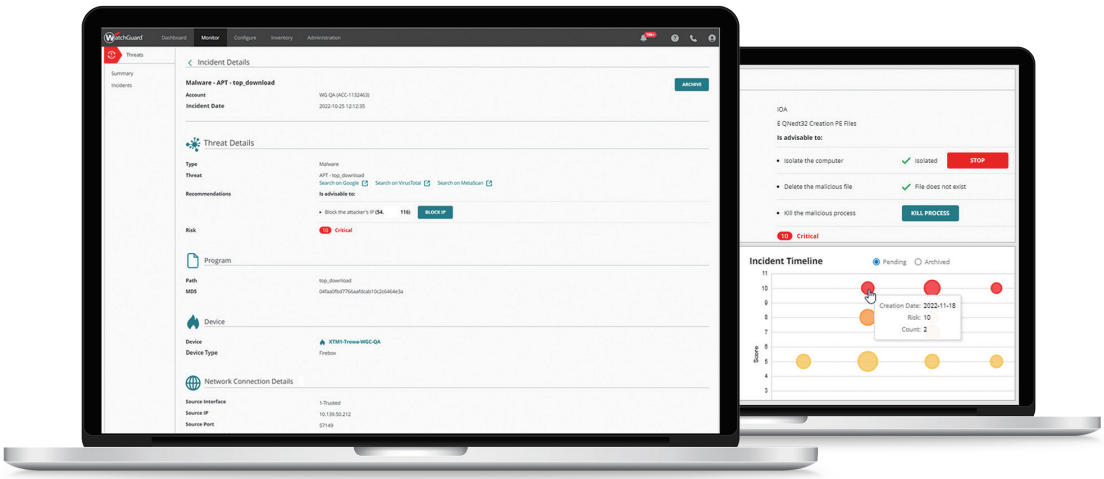
セキュリティオーケストレーション

セキュリティオーケストレーションと自動レスポンスを組み合わせることにより、組織はより包括的かつ密接したセキュリティ態勢を構築することができます。ThreatSyncは、複数のドメインからデータとアラートを統合し、インシデントコンテキストを生成し、レスポンスプロセスを合理化することにより、セキュリティチームは脅威に対してより迅速かつ効果的にレスポンスできるようになります。

主な機能

- セキュリティスタック全体から脅威データを自動的に集約することで、脅威を統合的に可視化し、検知時間の短縮と精度の向上を実現します。
- 異なるセキュリティソースより監視されているフィードを相関分析し、統合的な脅威検知で脅威を早期に発見することにより、MTTDを短縮することができます。
- 自動レスポンスとアラートスコアリングを統合し、手動での操作を避けることで、アラート疲れとMTTRの両方を削減します。
- セキュリティオーケストレーションにより、複数のプロセスやツールの連携と自動化を強化し、一貫したセキュリティ態勢を提供します。

XDRの詳細については、
ぜひウォッチガードの
Webサイトをご覧下さい



上の図は、インシデントと脅威の詳細、関係するエンドポイントとネットワーク、インシデントのタイムライン、
および有効なレスポンスアクションを示しています。

ウォッチガード・テクノロジー・ジャパン株式会社 〒106-0041 東京都港区麻布台 1-11-9 BPR プレイス神谷町 5 階
TEL：03-5797-7205　FAX：03-5797-7207　https://www.watchguard.co.jp　Email: jpnsales@watchguard.com