Secureworks®

Secureworks MDR for Microsoft：Microsoft E5からフルサービスのSOCへ

Microsoft E5のライセンスをフルサービスのマネージド・セキュリティ・オペレーション・センターに拡張

E5を導入しているMicrosoft®のお客様は、各自のライセンスから最大限のセキュリティ価値を引き出すとともに、投資対効果を可能な限り高め、最適なセキュリティ成果をもたらしたいと考えています。Microsoft®の戦略的セキュリティパートナーであるSecureworks®は、Microsoftのテクノロジーのあらゆる組み合わせに対応し、24時間年中無休の稼働も可能なフルサービスのマネージド・セキュリティ・オペレーション・センター（SOC）への補完や拡張を行います。

Secureworks Taegisプラットフォーム

Secureworks Taegis™は、マネージド・ディテクション＆レスポンス（MDR）ソリューションを強化する拡張ディテクション＆レスポンス（XDR）プラットフォームです。TaegisはMicrosoftとシームレスに統合し、Microsoftのほか、クラウド環境、メールシステム、IDシステムのようなビジネスアプリケーションなどのソースから監視データを収集して、脅威の予防、検知、リスク緩和、対応を実施します。Secureworksは、そのXDRテクノロジーや、Microsoftとの統合の実績のほか、ほとんどあらゆる脅威環境に対応するSOCを20年以上にわたって運用してきた経験を有します。

Microsoftと極めて広範に及ぶ統合を実現し、多種多様なサービスを備えたSecureworksでは、セキュリティの継続的な効率化を推進しています。現在、1,000社を超えるお客様が、Azure、Office 365、Active Directoryをはじめとする Microsoftのコネクターに Secureworksの統合を使用しています。
また、130万を超える Microsoft Defenderのエンドポイントで Secureworksが日々使われ、最高のセキュリティを実現しています。

SECUREWORKS TAEGIS XDRのメリット

- E5 Azure、Defender Suite、Office 365、Active Directory、Microsoft Sentinelなどで収集した監視データ
- あらゆる監視データを対象とする1年間のログ保持をすべてのお客様に提供
- MicrosoftやAzureベースのツールと簡単に統合
- 複数のベンダーが混在するEDR展開とも統合可能
- ベンダーの膨大な監視データを統合して可視性、検知性、的確性を向上
- カスタマーサクセスによる継続的な運用サポート
- 経験豊富な脅威マネージャーによる月1回の脅威管理アドバイザリーサービス
- TaegisのインターフェースからSecureworks SOCのエキスパートに90秒以内に連絡可能
- Taegisプラットフォーム内でインシデント対応チームがMicrosoft for Defenderエンドポイントの監視データを確認
- パッチチューズデーのインテリジェンスを適用
- Microsoft独自のランサムウェアおよびActive Directoryアセスメントを実施
- Windows NTハッシュ形式に対し、毎秒1兆回以上の推測が可能

最適なセキュリティ成果

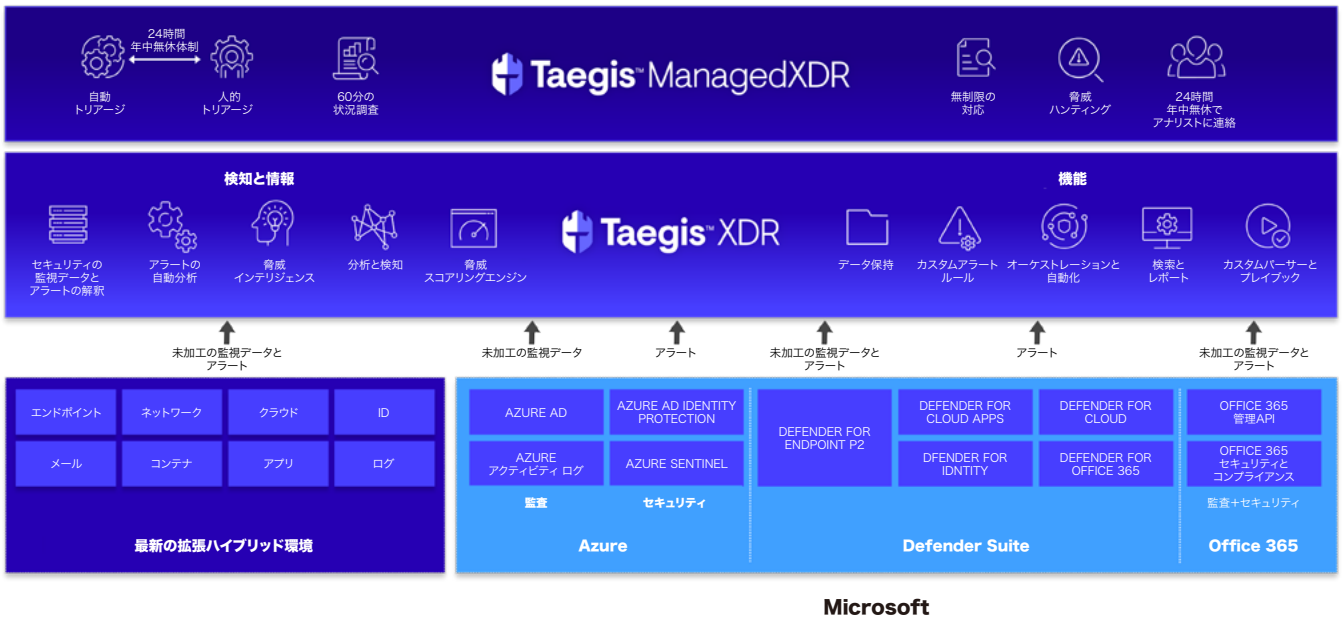
Secureworks Taegisは、迅速なオンボーディング、予測可能な運用コスト、脅威検知の自動化、最先端の脅威インテリジェンス、さらに以下の追加のソリューションで、メリットが得られるまでの時間を短縮します。

- 完全統合された脅威検知と対応管理で最適化されたセキュリティ
- SIEM型の監視データとログ機能
- 監視データの管理とエクスポート機能を備えた管理ポータルログアクセス
- 365日間(ローリング方式)の無制限の監視データ保持が標準で付属
- 定額の追加料金でログの保持期間を最大5年延長可能

IT環境がどれほど複雑でも、Microsoftにどれだけ多様な環境が相互接続されていても、Taegisは E5のライセンスにより幅広く対応し、セキュリティ面で多大なメリットをもたらします。

Secureworks Taegis と Microsoft の連携について

Secureworks Taegisは、拡張ディテクション＆レスポンス(XDR)を目的に構築されたSaaSプラットフォームで、SecureworksのSOCの専門知識とグローバルな脅威インテリジェンスを活用して、Microsoft向けのMDRとフルサービスのSOCを提供します。このために、Microsoft Azure、Defender Suite、Office 365のライセンスなどのMicrosoftのテクノロジーから最大限のセキュリティ価値を引き出して、E5ライセンスへの投資のROIを最大化します。



Secureworks Taegisは、Microsoftを始めとする多数のソースから監視データ、イベント、アラートデータをTaegis XDRプラットフォームに取り込みます。

Secureworks®

Secureworks Taegisは、充実した脅威インテリジェンスや、ウォッチリストなどの重要な検知情報を収集し、高度な分析エンジンと検知エンジンで処理します。そして、脅威を「情報」から「クリティカル」の5段階に適切に分類し、誤検知を最小限に抑えながら、用意された何千もの対策プログラムとプレイブックをもとに、分類に応じた検知アラートと対応を自動的に生成します。お客様は、各自の環境に合わせてルールやプレイブックをカスタマイズすることや、Secureworks SOCのアナリストに協力を仰ぐことができます。Taegisは綿密なレポートやログを生成し、あらゆるITおよびOT環境にわたる脅威や攻撃を詳しく理解できるようにします。

目標はシンプルで、脅威が生産性やブランドの評判を損いかねない攻撃になる前に認識して対応し、緩和することです。Microsoft Securityによるエンドポイント、クラウド、Office 365アプリケーションからのデータのほか、IDシステムや他のビジネスアプリケーションなど、他のシステムのデータを使用して、お客様はこの目標を実現できます。

Secureworksがサードパーティのサイバーセキュリティポイントソリューションの監視データを分析したところ、ポイントソリューションで「高」または「クリティカル」として生成されたアラートのうち、高度な検知インテリジェンスを備えたTaegisが「高」または「クリティカル」とみなしたのはわずか1.3%でした。

つまり、Taegisを使用するサイバーセキュリティアナリストは、信頼性の低い98.7%のアラートではなく、まさにクリティカルな1.3%のアラートだけにすぐさま対応すればいいということです。

Secureworks®

SECUREWORKS TAEGIS FOR MICROSOFTのメリット

ITおよびOTスタック全体にセキュリティ防御を拡張

攻撃者は、防御の隙を突いてきます。Microsoftのお客様がSecureworks Taegisを使用すれば、LinuxやmacOSの展開を含め、異常な動作がどこで発生しても検知して対応することができます。また、他のセキュリティツールやITアプリケーションでも、Taegisの数百種類に及ぶセキュリティ統合で対応できます。

Microsoft向けに最適化

SecureworksはMicrosoftとセキュリティの戦略的なパートナー関係を結んでおり(「Microsoft 365 Defenderでサポートされるプロフェッショナルサービス | Microsoft Learn」を参照)、検知や対応の価値を最大限に高めるためにMicrosoftとの統合を継続的に更新しています。Microsoftを使用しているTaegisのお客様の60%が、他のEDR(Taegis MDRに付属するTaegisエージェントを含む)を1つ以上使用しています。Secureworksは、他の大手のEDRベンダーとの統合も維持しているため、どのEDRでも機能します。

30日の迅速な展開

世界各地に何千ものお客様が存在するSecureworksでは、カスタマーサクセスチームと脅威エンゲージメントマネージャーがガバナンスとサービスライフサイクルのサポートを実施しています。この両者が協力して運用上のセキュリティ管理目標が確実に達成されるように、定期的にレビューを実施し、セキュリティ上の重要な判明事項やセキュリティ体制の強化に向けた詳しい推奨事項をお客様に伝えています。

攻撃者の手口を詳細に追跡

Secureworksには、175を超える脅威グループを監視する専任の脅威インテリジェンス調査チームが存在します。この情報は、400億種の脅威インテリジェンスをまとめた独自の脅威グラフに取り込まれます。Taegisはこのインテリジェンスを活用して脅威を迅速に検知し、サイバーセキュリティポイントソリューションが見逃しがちなリスクを捉えます。

Azure、Defender Suite、Office 365を統合

Taegisは、エンドポイント、クラウド、IDシステム、Office 365などからアラートや監視データを取り込んで分析します。お客様はMicrosoft E5のライセンスから最大限の価値を引き出すことができます。

予測可能な一括価格設定

Secureworks Taegisソリューションは、エンドポイント単位で一括の価格が設定されており、不明瞭な追加料金がありません。Microsoft E5のライセンス数、他のEDRソリューション、追加する必要があるエンドポイントのライセンス数を提示するだけで、Secureworksのパートナーから正確な見積もりを得ることができます。他のソリューションとは異なり、データ量によって追加料金が課されることもありません。また、365日間の無制限の監視データの保持が付属しますが、Microsoft Sentinelや他のMDR/XDRプロバイダーの場合は90日以下です。

SecOps担当者のストレスや負担を軽減

Taegisの極めて重要な利点は、SecOpsチームが迅速か簡単に脅威への警戒をできるようになること、そしてその警戒を持続できることです。Taegisでは、重要性の高い検知が何千件もあらかじめ用意されているほか、追加の設定なしで偽検知を大幅に減少させるTTPやMITRE ATT&CKによる高度な検知も行うため、チームが無駄な調査に時間を浪費することがありません。

透明性、完全性、コラボレーション

Taegisは、セキュリティアナリストのために、セキュリティアナリストとのコラボレーションを念頭に設計・構築されています。お客様と当社のアナリストが同じプラットフォームで同じデータを確認するため、透明性が格段に高まります。Taegisでは、最先端のテクノロジーを活用し、世界各地のセキュリティエキスパートとともにお客様と連携して、市場の他のどのセキュリティ運用管理ソリューションよりも優れたセキュリティ成果をもたらします。

Secureworks®

Secureworks®(NASDAQ:SCWX)は、SaaSベースのオープンXDRプラットフォームSecureworks® Taegis™を通じて人類の発展を守る、サイバーセキュリティのグローバルリーダーです。20年以上にわたる実際の検知データ、セキュリティ運用の専門知識、脅威インテリジェンスとリサーチに裏打ちされたTaegis™は、AIを活用した高度な脅威の検出、インシデント調査の効率化とコラボレーション、適切なアクションの自動実行を実現し、世界中の数千を超える組織のセキュリティ運用に組み込まれています。

詳細は、当社のセキュリティスペシャリストにご相談ください。
☎03-4400-9373
secureworks.jp

©2024 Secureworks, Inc. All rights reserved. Availability varies by region.