DATA SHEET

Taegis™ XDR（テイジスXDR）

自動化、機械学習ベースの分析機能、
包括的な脅威インテリジェンスによる高度な脅威の
防止・検知・対応

先手を打って攻撃者に対抗

サイバー攻撃の巧妙化、ステルス化に伴い、多くの企業や政府機関は後れを取るまいと悪戦苦闘しています。ハイブリッド型IT環境の死角、セキュリティチームの人員不足、散在するセキュリティツールの管理コストや複雑性の増大などの問題を抱える組織には、eXtended Detection and Response（XDR）ソリューションが必要です。XDRソリューションは既存のセキュリティインフラを統合し、実用的で的確な知見を導き出すと共に、単一コンソール上で高度なオートメーション機能を駆使して脅威を調査し、迅速に対応します。

22年にわたって業界をリードしてきたセキュアワークスの原動力であるセキュリティオペレーションのノウハウや脅威動向に関する豊富なナレッジが集約されたクラウドネイティブ型のSaaSプラットフォーム「Taegis XDR」が、皆様のセキュリティオペレーションの効果・効率を高めます。

- お客様組織のセキュリティファブリック全体で収集した監視データを集約し、エンドポイント、ネットワーク、クラウド環境すべてを可視化してコントロール
- AIを駆使した分析および、セキュアワークスのカウンター・スレット・ユニット™が生成した包括的な脅威インテリジェンスで高度な脅威を検知
- あらゆるデータ、脅威ハンティングツール、自動対応プレイブックが集約された使い勝手の良いクラウド型コンソールの単一画面で、調査とインシデント対応をスピードアップ

主な特長

- エンドポイント、ネットワーク、クラウド環境をはじめとする攻撃対象領域全体をカバー
- 攻撃手法の異なる監視データやイベントを機械学習／深層学習ベースで解析し、包括的な脅威インテリジェンスを適用して深掘り
- 必要な情報やデータすべてが適時・適所に反映された高精度のアラート
- ワンクリックで実行可能な対応アクションと自動プレイブック
- 外部セキュリティツールとの広範囲な統合連携（プリ・インテグレーションでのご提供に加え、容易にカスタム統合可能なXDRのオープンソリューション）

Availability varies by region. ©2021 SecureWorks, Inc. All rights reserved.

セキュリティ効果を最大化

既知および未知の脅威の防御・検知・対応

- 多くの組織にとって通常、最初の防衛線はエンドポイントです。Taegis XDRには、Taegis NGAVの強力な次世代エンドポイント脅威防御機能と、Taegis EDRが広範囲なエンドポイントから遠隔収集した監視データが一体化されています。そのため、エンドポイント環境に出現した脅威の大半を撃退できると同時に、エンドポイントに関する詳細な情報にもとづき脅威をきめ細かく調査できます。

- Taegis XDRは、お客様組織のネットワーク、クラウド、エンドポイント、各種セキュリティツールで収集されたシグナルを、厳選された脅威インテリジェンスと統合します。そのため、攻撃対象領域全体を単一画面で可視化してコントロールできます。

- AIを駆使したTaegisの検知機能が、最先端の機械学習アルゴリズムおよび分析手法を活用して対象環境における悪意ある活動の発生有無を常時監視し、攻撃者の振る舞いを早期に認識します。Taegis XDRの自動対応プレイブックおよびワンクリックの対応アクションにより、対応をスピードアップできます。Taegisは、高度な攻撃が実害に発展する前に攻撃を検知、把握、阻止するための製品です。

攻撃者の意図および振る舞いを理解

- セキュアワークスのカウンター・スレット・ユニットが常時生成する包括的な脅威インテリジェンスを用いて新たな脅威および攻撃者の意図や振る舞いを細部にわたって解析し、当社のナレッジが反映されたTaegis XDRの対抗策を用いて攻撃を撃退します。さらに、脅威に関する基本項目（攻撃者の身元、攻撃の内容、発生時間、発生理由、攻撃手法）の解析時にも当社のインテリジェンスをご活用いただけます。

セキュリティオペレーションの効率アップ

重要なインシデントを確実に調査

- お客様組織のセキュリティファブリック全体をカバーするTaegisが、複数のセキュリティツールから収集された脅威インテリジェンス、ログおよびイベントを相関付けし、アラートの検証および優先度分類を行います。その結果、貴社アナリストは誤検知の対応に追われることなく、余裕をもって「真の脅威」に対処できます。

攻撃の謎をいち早く解明

- Taegisは、お客様組織のエンドポイント、ネットワーク、クラウド環境全体で関連性のあるイベントを自動で相関付けします。この情報を、脅威シナリオの全容解明および、攻撃の根本原因の早期特定にお役立ていただけます。

Taegis XDRのメリット

防御・検知・対応の一元化

受賞歴のあるTaegis XDRの検知・対応機能と、Taegis NGAVの次世代エンドポイント脅威防止機能が一体化された直感的かつ包括的な防御・検知・対応ソリューションです。

脅威をより迅速かつ正確に検知

エンドポイントから侵入する脅威をTaegis NGAVが自動で阻止します。また、セキュアワークスのカウンター・スレット・ユニット™が生成する脅威指標、対抗策、個別分析項目をもとに常時更新されるTaegis XDRの高度な分析エンジンがお客様環境の至る所で高度な攻撃を検知します。実証済みかつ優先度分類済のアラートをもとに「真の脅威」をいち早く特定できるため、誤検知対応に追われずに済みます。

セキュリティオペレーションの最新化

Taegis XDR上でセキュリティインフラ全体を可視化し、あらゆる調査を一元的に実施できるため、手作業でデータをつなぎ合わせたり複数のツールを使い分ける必要はありません。年間1,400件を超える当社のインシデント対応案件のノウハウが反映された対応アクションのレコメンデーションおよび自動対応プレイブックを活用することで、平均修復時間（MTTR）を数分単位に短縮できます。

Availability varies by region. ©2021 SecureWorks, Inc. All rights reserved.

Secureworks

あらゆる調査を単一プラットフォームで実施

- お客様環境全体のデータをTaegisに集約し、包括的な脅威ハンティングのツールキット（MITRE ATT&CKのTTPなど）を適用します。したがって、貴社アナリストはセキュリティインフラの全体像を把握でき、Taegisプラットフォーム上であらゆる調査を実施できます。データを手作業でつなぎ合わせたり、複数のツールを使い分ける必要はありません。

脅威をエンドポイントでブロックし、リスクを低減

- Taegis NGAVは、標的型攻撃や新種の攻撃を含むほぼすべてのサイバー攻撃をエンドポイントで自動阻止します。これにより侵害リスクを低減しつつ、調査対象となる脅威の件数を絞ることができます。その結果、エンドポイントを突破する脅威の数が減り、担当アナリストの工数を「より高度かつ重大な脅威の対応」に振り向けられる、などの効果を期待できます。

チームワークでより賢く、迅速に

- 柔軟性にすぐれた検索・レポート作成機能が搭載されているため、関連情報を担当アナリストが素早くまとめ、チームメンバーと共有しながら調査におけるコラボレーション（コメントの挿入、関連データの追加/削除、ステータス変更など）を促進できます。これにより、コラボレーションの効率や意思決定のスピードが改善し、調査の作業をスピードアップできます。

セキュアワークスの専門家にその場で相談

- セキュリティアラートやワークフローに関して担当アナリストやご利用者が困っている、または調査のサポートが必要な場合はTaegisコンソールから直接、わずか60秒で当社の専門家にご相談いただけます。当社サービスのご利用有無は問いません。

「Taegis NGAVは成熟した製品であり、小規模な環境から多国籍企業まで様々な導入形態に対応できます」

「安定した性能で、実際に出回っているマルウェアを確実に検知し、すぐにSOCに実装可能なコンソールや機能を備えたSecureworks Taegis NGAVがITセキュリティ対策のラインアップに加われば心強いでしょう」

MRG Effitas Efficacy Assessment Report

Availability varies by region. ©2021 SecureWorks, Inc. All rights reserved.

Secureworks

Secureworks Taegis XDR のハイライト

22

セキュリティサービスと脅威リサーチにおいて、22年にわたり市場を牽引してきたセキュアワークスの実績をもとに構築

246

セキュアワークスが監視する攻撃グループの数

60秒

調査のサポートが必要な場合、わずか60秒でセキュアワークスの専門家にコンタクト可能

90%以上

MITRE ATT&CKに掲載されているTTPの90%超をカバー

「当社では毎月20億件ほどのイベントが生成されますが、Secureworksを使えばこの数を20～30件程度に絞り、高精度なアラートを抽出できます。おかげでチームは大助かりです」

サイバーおよび情報セキュリティ部門ヘッド
Sunil Saale氏

Secureworksについて

SecureWorks® (NASDAQ：SCWX) は、20年以上にわたり実環境で蓄積された脅威インテリジェンスとリサーチに基づき構築されたクラウドネイティブのセキュリティ分析プラットフォームSecureworks® Taegis™により、高度な脅威の検知、合理化された協調モデルによる調査、また脅威に対する適切なアクションを自動的に実施する能力を強化し、お客様のビジネスを保護するサイバーセキュリティのグローバルリーダーです。

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

Availability varies by region. ©2021 SecureWorks, Inc. All rights reserved.