

セキュリティ・イベント監視サービス

脅威インテリジェンス主導型のリアルタイムな監視により、脅威に対する検知、防御、対応能力を強化

大量のログ・データへの対応

今日のサイバー・セキュリティ攻撃と闘うためには、適切なセキュリティ機器、情報、経験が必要ですが、それは簡単ではありません。サイバー攻撃を防御、検知し、対応する能力を強化するには、IT 環境全体を十分に可視化することが必要となります。セキュリティ担当者は、大量のログ・データから何が本当の脅威であるかを判断し、さらに迅速かつ効果的にそれに対応しなくてはなりません。ほとんどの組織では、24 時間365日常時、十分に整備されたセキュリティ対策を維持するだけの予算や時間はなく、また専門的な知識を持つ担当者もいません。その結果、組織のインフラを強固にするのには、ヒューマン・インテリジェンス (HI) と人工知能 (AI) とを組み合わせた事前対策が必要ですが、それにはほど遠い状況です。

Secureworks が解決します

Secureworks のセキュリティ・イベント監視サービスは、お客様の環境で現在起きているイベントをリアルタイムに監視、相関分析を行い、さらに専門家による分析も実施します。Secureworks のカウンター・スレット・プラットフォーム (Counter Threat Platform™:CTP) を活用し、人工知能とヒューマン・インテリジェンスを強力に組み合わせることで、お客様のセキュリティ・オペレーションの統合、簡素化を支援します。

数十億のイベントデータ拠点、世界中で 4,400 のお客様を日々監視する中で得たデータや、Secureworks のカウンター・スレット・ユニット (Counter Threat Unit™ :CTU™) のリサーチ・チームによって可視化された世界規模の脅威情報に基づき、Secureworks のセキュリティ・イベント監視サービスでは、お客様が脅威の状況をより理解し、それに迅速に対応することを支援します。Secureworks のセキュリティ・オペレーション・センター (SOC) には経験豊富なリサーチャー、アナリスト、エンジニア、コンサルタントが在籍し、お客様にとって、真の脅威となり得るイベントへの継続的な調査を行います。

包括的な脅威インテリジェンス、予測技術、セキュリティ専門知識の力

Secureworks のセキュリティ・イベント監視サービスは、お客様が脅威の状況をより理解し、迅速な防御、対応を可能とする目的で設計された包括的なセキュリティ対策サービスです。Secureworks の CTU は、法的執行機関やセキュリティ関連団体との何百ものネットワークや、70人以上のセキュリティ・リサーチャーの専門知識、ダークネットの調査で得られる情報等を駆使することで、常に進化を続ける脅威動向への比類なき可視性を維持しています。当社の CTU は市場に先駆けて最新の脅威と脆弱性に関するソリューションを提供しています。

お客様のメリット

- ネットワーク、エンドポイント、アプリケーション、クラウド全体にまたがる可視性の統合
- 誤検知を減らし、本来のビジネスの重要事項に注力
- 既存のセキュリティ投資への投資利益率 (ROI) を最大化、およびお客様にとって最適なテクノロジーの選択、投資
- セキュリティ知識不足の解消
- 最新の脅威インテリジェンスとともに、修復方法に関する実用的なガイダンスの入手
- 相関分析と機械学習を活用した高精度なイベント検知および分析の自動化
- 柔軟な分析と可視性を備えたツールを使用し、カスタマイズされたレポートを利用

カウンター・スレット・プラットフォームでは、マシン・インテリジェンスを活用し、検知したイベントの 99.99 % 以上を自動的に処理します。

さらに、セキュリティの専門家が24時間365日 常時、調査や修復のための助言などのサポートを提供しています。

お客様ポータルで提供する分析機能は、お客様がリスクを理解し、また、コンプライアンス遵守の実証や、お客様の環境の比類なき可視性を実現を支援します。モバイル・アプリケーションを利用すれば、外出先でもこの情報を確認することができます。



19+

年蓄積したサイバー・スレット・インテリジェンス



2,500億

日々処理するセキュリティイベント



4,400

ワールドワイドのお客様



300+

熟練のセキュリティ・アナリスト

本サービスの重要性

強力な最新のインテリジェンス：

Secureworks の CTP はお客様の実環境において約 3,000 億のイベントを日々処理しており、CTU リサーチ・チームはインターネット上の脅威を洗い出し、あらゆる技術、業界、環境などにまたがる脅威動向への深い洞察を提供します。

専門家による 24 時間 365 日 常時システムおよびデータの保護：

Secureworks がお客様のインフラを 24 時間監視するため、お客様はセキュリティ専門の担当者を雇用、訓練し、またその技術を維持する必要がありません。

既存のサイバー・セキュリティ対策への投資価値を有効活用：

Secureworks の CTP はログを生成することのできるデバイスであれば独自技術を使用したデバイスであってもほぼ監視することができるため、お客様の既存のセキュリティ対策を有効活用しながらもお客様のデータ保護を支援します。

サービスの特長

- ベンダー・ニュートラルな監視プラットフォーム：主要ベンダー・テクノロジーを網羅
- 人工知能とヒューマン・インテリジェンスを活用した 24 時間 365 日の監視により、攻撃に対する有効性の高い検知を実現
- 最新の脅威インテリジェンスを活用した強力な相関分析
- グローバルの脅威動向への非常に優れた可視性
- コンプライアンスの遵守体制を実証するための詳細なレポート機能

Secureworks について

グローバルのサイバーセキュリティ・サービス業界をリードする Secureworks® (NASDAQ: SCWX) は、デジタル化が進む社会において、企業組織をサイバーの脅威から保護し続けています。

当社は、数千社におよぶお客様から集積したデータと人工知能 (AI)、そして独自のカウンター・スレット・プラットフォーム (Counter Threat Platform™ : CTP) の自動化による可視性と、お客様の環境を保護する強固なネットワーク効果を創出する当社の卓越したリサーチとアナリスト集団から提供される実践的な分析結果を統合してサービスに反映させます。

データの種別や出所を問わず集積・分析を行うことで、セキュリティ侵害の防御、悪意ある活動のリアルタイムによる検知、深刻化する脅威の迅速な対応と予見を実現し、サイバーの脅威への対抗策をお客様に提供します。

もっと上手に組み合わせれば、セキュリティは飛躍できる™



より詳細な内容に関しては、下記のメールアドレスにご連絡ください。

SCWX_PreSales@secureworks.com

代表 03-6893-2317

secureworks.jp

SecureWorks Japan 株式会社