YOKOGAWA

Co-innovating tomorrow™

OpreX™ Safety and Security

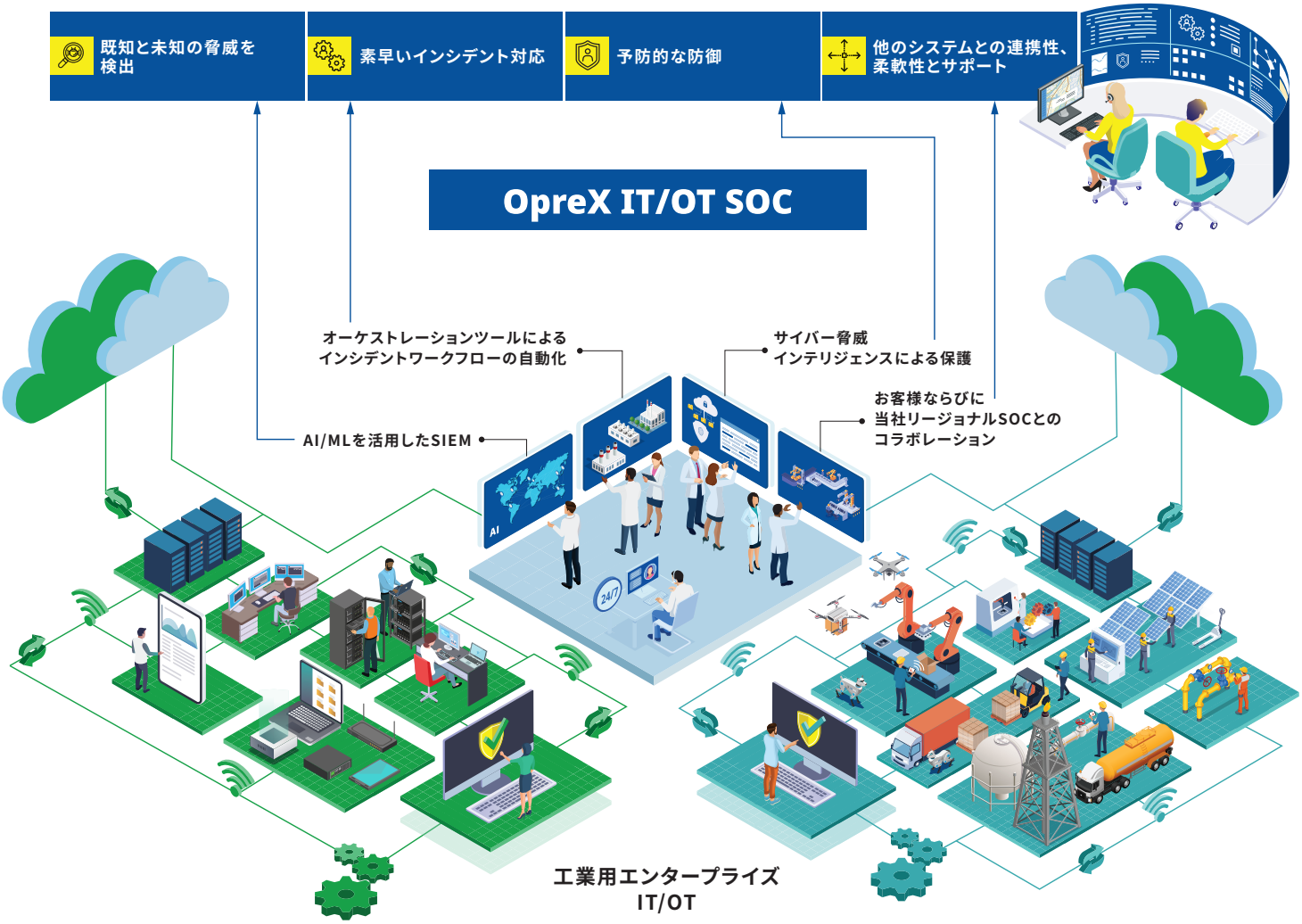
OpreX™ IT/OT Security Operations Center (SOC)

BU89A01A03-02JA

OpreX IT/OT Security Operations Center (SOC)

OpreX IT/OT SOC は、IT環境に加え、業務上必要不可欠なOTシステムと、ネットワークの可用性および完全性の監視と先見的な保護を容易にできるようにし、安全なオペレーションを支援します。

統合化されたプロセス、自動化されたワークフローとテクノロジー、認証資格を有するセキュリティエキスパートとR&Dスペシャリストのチームからなる、OpreX IT/OT SOCは、企業のITとOT双方のセキュリティシステムとネットワーク全体を可視化し、インシデントや脅威の効果的かつ継続的な検知・分析・対応に必要な複数の3要素（人材・プロセス・テクノロジー）を統合するオーケストレーションツールです。



ITネットワークのセキュリティ監視

リアルタイムの監視

OTネットワークのセキュリティ監視

付加価値のあるダッシュボード

既存のSOCに代えて

さまざまな製造業への対応に特化した OpreX IT/OT SOCは、単独で自律的に稼働し、隔離された、自己完結型で専用のソフトウェアで稼動していることの多いOTシステムも保護の対象です。また、企業のセキュリティ状態を単一のツールでリアルタイムに監視できる、ITとOTのセキュリティセンターを兼ね備えた、バランスの取れた先見的なモデルです。

統合された一貫性のあるセキュリティ対策は、OpreX IT/OT SOCにお任せください。

AI/MLを活用したSIEMによる未知の脅威の検出

異常なアクティビティや高度な攻撃を、素早く警告し、解決します。

迅速な対応のための自動化ワークフロー

人的ミスを最小限に減らすため、タスクを連携、実行、自動化して、迅速に解決します。

常時監視・保護

サイバー脅威インテリジェンスを用いて、ログ情報・イベント情報を絶えず収集・調査することで、疑わしいアクティビティをリアルタイムで検出します

既存のインフラとシームレスに統合

既存のセキュリティシステムやデータ管理システムと OpreX IT/OT SOCを簡単に統合できます。

企業におけるセキュリティの課題を解消する IT/OT SOCサービス

サイバーセキュリティに関するリスクの管理は新たな時代に突入しました。働き方が変化を続け、システム間の接続がますます増えるなかで、サイバーセキュリティの脅威に関する状況も変化しつつあります。こうした環境において、多くの企業はセキュリティ・オペレーション・センター（SOC）を立ち上げ、迅速な対応と確かな修復を行うことで、セキュリティに関して生じるリスクを軽減しようとしています。

OpreX IT/OT SOCは、製造業固有の課題への対応を容易にします。

- ソフトウェアやオペレーティングシステムが最新の状態でなかったり、パッチが適用されていなかったりすることによる脆弱性を迅速に特定
- IT環境とOT環境間の適切なネットワークセグメンテーションを支援
- 物理的アクセス制御およびデジタルアクセス制御の支援
- デジタルSOCプレイブックの提供による、リスクの検知・対応ワークフローおよび対応プロセスの向上
- セキュアなコンフィギュレーション管理および方法の支援

OpreX IT/OT SOCの仕組み

OpreX IT/OT SOCは、サイバー脅威インテリジェンス（CTI）と機械学習（ML）プログラムの双方を駆使して、IT/OT環境全体のDNS/ADサービス、侵入検知システム、工場システムなどの監視を容易にする専用のソリューションです。

当社は、人材・プロセス・テクノロジーと、ガバナンス・リスク管理・コンプライアンスを統合し、包括的で持続可能な価値を生み出します。

人材

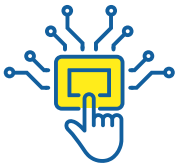
チームの強化

当社の包括的な専門知識を利用した、トレーニングやワークショップ、社内スキルの構築、職務と責任の明確化により、セキュリティに対する態勢の向上のお手伝いをいたします。

プロセス

革新を目指したワークフロー設計

チケットシステムを通じ、お客様の業務の構造、プロセス、問題点を十分に把握し、吟味したうえで、適切なワークフローを作り上げます。



テクノロジー

基幹業務用データのための堅牢なプラットフォーム

単一ウィンドウ表示のIT/OT SOCダッシュボードは、アラートやインシデントを監視し、工場のリアルタイムデータに基づく迅速な意思決定を行ううえで、信頼できる情報源です。

当社のIT/OT SOCのセキュリティフレームワークは5段階構成です。

事後対応

1 境界型セキュリティ

- 防御計画
- パッチプログラム
- ファイアウォールおよびエンドポイントセキュリティ
- 手動による修復

2 SIEM/データレイクの移行

- セキュリティ状態ログの取得
- ログの集約および取得
- ユースケースエンジニアリング
- EDRの実装

事前対応

3 高度な分析

- 脅威に関する情報に基づいた検索
- ML活用した分析
- 脅威ハンティング
- 調査、フォレンジック、IR

4 セキュリティのオートメーション

- SOARの導入
- インシデント処理のオートメーション化
- 統合型ツール
- 攻撃タイプに応じたプレイブック

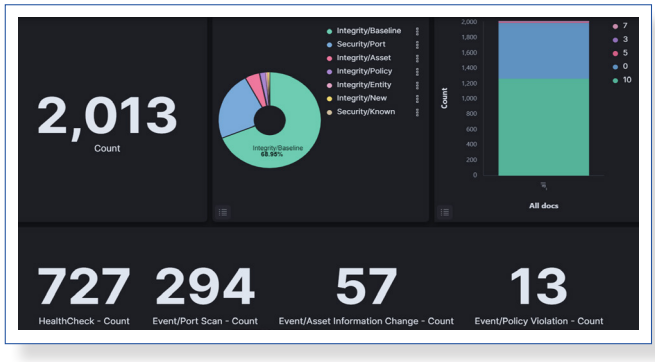
5 予測分析

- 可能性の高い攻撃経路の特定
- 敵対的シミュレーション
- 内部脅威検知
- エンドツーエンド自動化

新たなレベルのセキュリティコントロール

OpreX IT/OT SOCは、強力なAI・MLにより、組織全体から収集した複雑なセキュリティデータをカスタマイズ可能で、ユーザーフレンドリーなダッシュボードに表示します。お客様ごとに、業務上の要件に基づいて設計・配置を行い、オープン　アーキテクチャを介して重要なテクノロジーコンポーネントと統合します。

IT/OT SOCダッシュボードのスクリーンショット



1. AIを活用したクラウドベースのSIEM
2. サイバー脅威インテリジェンス（CTI）スイート
3. 検知プログラム
4. ネットワーク侵入検知システム（NIDS）
5. インシデント管理

充実したIT/OTセキュリティサービス

SOCスタートアップサービス

お客様のリスクに応じて、監視ログやイベント情報の決定を行います。（お客様のセキュリティ対策機能が不十分の場合はセキュリティリスクの提言は追 加セキュリティ製品のアドバイスをさせていただきます）ログ収集には、syslog転送とサーバにログ収集Agent（Beats）をインストール、更にSaaSとのAPI連携な の方法があります。お客様の状況に応じて選択可能です。

IT/OT SOC監視サービス(年間契約)

各種機器のログ、イベント情報から不正アクセスやマルウェアなどのセキュリティ監視を行い、インシデントレポートを提供します。アラート一覧は、インシデントダッシュボードから内容を確認できます。隔週または月次の定例会により監視内容をご説明します。またリスク軽減や対処方法についてアドバイスさせていただきます。月次、四半期毎のレポートにより、リスクトレンド分析を行います。

インシデント対応トレーニング

監視対象のシステムの各種アラート情報に対してPlaybookをご提供し、リスクの軽減や対処方法についてインシデントトレーニングプログラムを提供します。お客様セキュリティインシデントレスポンスチーム(CSIRT)が、インシデント分析、リスク軽減活動を行うための標準化されたオペレーション手続き(SOP, Standard Operation Procedure)の教育を提供します。

アセスメントサービス

YOKOGAWAのセキュリティアナリストがネットワークやアプリケーションの脆弱性を評価し、改善策を提案いたします。ターゲットに対して外部から模擬的に攻撃を加えるペネトレーションテスト（Pen Test）や、データやログ・通信データなどの情報をもとに評価する脆弱性診断（VA）をおこないます。

フォレンジックサービス

セキュリティインシデントが発生した際に、YOKOGAWAのセキュリティアナリストが原因と影響範囲を調査し、封じ込め策や予防策を提案します。解析対象の違いに応じて、ハードディスクのイメージデータや実行ファイル・データファイルを解析するコンピューターフォレンジック、また通信パケットを解析するネットワークフォレンジックをおこないます。

当社のセキュリティコミットメント

当社は、お客様に卓越したセキュリティと安全性を提供することをお約束します。当社のエンジニアは、最高のグローバルセキュリティ基準を満たせるように常にトレーニングを受けています。

025-0005-40

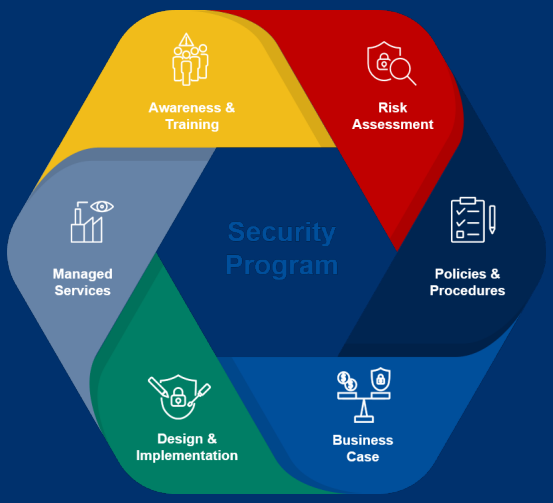
本サービスは、経済産業省が設ける「情報セキュリティサービス基準審査登録制度」に基づき、第三者機関により認定されたサービスです。

世界規模のセキュリティネットワーク

当社が提供する世界規模のセキュリティ・オペレーション・センターのネットワークは、世界各地に広がり、協力して専門知識やベストプラクティスを共有することで、堅牢なサイバーセキュリティを飽くことなく追求し、お客様に包括的な情報、セキュリティ態勢の向上、対応の迅速化、レジリエンスの向上などのメリットをもたらします。

YOKOGAWA's Security Program

企業には、それぞれ独自のセキュリティ要件が あります。そのため、当社のコンサルティング主導 では、必ず最初に、自社のリスク特性の把握および 数値化、重要なデータ資産の特定、現在のセキュ リティ戦略と保護レベルの評価をお客様が行う お手伝いをいたします。



OpreX IT/OT SOCは、数十年に わたって蓄積された、製造業のオ ートメーション化 に関する専門知識、サイバーセキュリティアーキ テクチャ設計のベストプラクティス、安全性と セキュリティを担保するプラントおよびオペレ ーションに関する知識に基づいて構築されました。レジリエントなサイバーセキュリティのサービス およびソリューションにより、プロセス産業における サイバーリスクの軽減を目指す、当社が提供するSecurity Programのひとつです。

OpreX IT/OT SOCは、管理サービスとして提供されるた、タイムリーなセキュリティアップデートや セキュリティ性能の継続的な監視ができるようになり、企業のセキュリティを最高レベルに保つという根本的な 課題を解決します。

今すぐ始めましょう

当社は、100年以上にわたるOT分野での豊富な経験を活用し、計測、制御、セキュリティなどの分野における革新をもたらす、先進的なテクノロジーを提供してきました。

詳細については、当社のウェブサイトをご覧ください
(https://www.yokogawa.com/jp-ydj/solutions/services/oprex-itot-soc/)

横河ソリューションサービス株式会社
横河デジタル株式会社
〒180-8750 東京都武蔵野市中町2丁目9-32
https://www.yokogawa.com/jp-ydj/

ウェブサイト:
https://www.yokogawa.com/jp-ydj/solutions/services/oprex-itot-soc/

お問い合わせは

Printed in Japan, 212(VC) [Ed:01/b]

YOKOGAWA Co-innovating tomorrow™