セキュリティ監視および対応により、レジリエンスを構築し、OTサイバーセキュリティ体制を強化

急速に拡大する今日のデジタル環境において、制御技術(OT)のインフラの保護はこれまで以上に重要になっています。

サイバーリスクが増大し続ける中、製造業は進化する脅威に先手を打つために、常に警戒を怠らず、専門知識を駆使する必要があります。セキュリティ監視および対応は、OTサイバーセキュリティ体制を強化し、サイバー脅威に対する強固な保護を提供する包括的なセキュリティサービスです。

産業組織は重大なサイバーセキュリティの課題に直面しています。

サイバー攻撃の高発生率: 過去1年間に産業組織の約70%がOTサイバー攻撃を経験しました(出典: Palo Alto Networks)。

限られたリソース: 多くの組織では、脅威の活動を継続的に監視し、セキュリティアラートを分析し、インシデントに効果的に対応するための社内リソース、専門知識、時間が不足しています。

脅威の優先順位付け: OT環境を標的とするサイバー脅威は進化しており、組織は脅威アラートに圧倒され、実際のセキュリティリスクを適切に特定し、優先順位を付けて対応することが困難になる可能性があります。

セキュリティ監視および対応の概要

セキュリティ監視および対応は、産業組織にOT環境を年中無休24時間体制でリアルタイムで監視し、脅威の検知、優先順位付け、対応を可能にします。これにより、コンテキストに基づいた脅威インテリジェンス、リスクに基づく優先順位付け、そしてOTに特化したセキュリティ分析が可能になり、アラート疲れを解消し、真の脅威が業務に影響を与える前に対処できるようになります。

従来のセキュリティソリューションとは異なり、セキュリティ監視および対応はOT環境に特化して設計されており、単一の拠点からグローバル企業全体にわたる既存のOTインフラにシームレスに統合されます。当社のOTセキュリティ・オペレーション・センター(SOC)に支えられたセキュリティ監視および対応は、リスクを未然に防ぐために必要な可視性、専門知識、そして迅速な脅威対応を実現します。

1. 脅威の早期検知と軽減により、混乱、ダウンタイム、潜在的な経済的損失を最小限に抑えます。
2. セキュリティ状況をリアルタイムで可視化することで、データに基づいた意思決定を可能にします。
3. 日々のセキュリティタスクを自動化することで、運用効率を向上させます
4. 専任のセキュリティチームが顧客チームの延長として機能し、スキルギャップを補います。

主な機能

継続的な監視と高度な脅威検知

年中無休24時間、リアルタイムの監視と潜在的な脅威の迅速な検知を実現します。高度な分析と専門家による分析により、アラートの優先順位付けと分析を行ない、最も重要な問題に優先的に対処できます。

迅速な対応と修復

セキュリティインシデント発生時に迅速な対応を行なうための専門家のガイダンスを提供します。SOCアナリストは、対応が必要なインシデントをエスカレーションし、効率的な管理のための段階的なサポートを提供することで、運用への影響を最小限に抑えます。

包括的なレポートと拡張性

包括的な月次エグゼクティブサマリと四半期ごとのビジネスレビューを提供し、ステークホルダーへの情報提供とエンゲージメントを強化します。モジュール式で拡張性の高いソリューションは、お客様それぞれのニーズに合わせてカスタマイズされ、柔軟性と成長を実現します。

テクノロジの概要

セキュリティ監視および対応は、業界をリードするテクノロジと専門知識によって提供されます。

グローバルOT SOC: ティアおよび2のSOCアナリストを配置し、年中無休24時間体制の継続的な監視を提供します。

OT SOCプラットフォーム: 自動化されたプロセス、OT脅威ルール、高度な分析、OT/IT脅威インテリジェンスを活用し、OT環境の脅威アラートを状況に合わせて解釈し、より迅速な対応を可能にします。

サイバーセキュリティリード: 専任のSOCアナリストが、お客様の特定の環境に関連する潜在的な脅威に関する洞察とインテリジェンスを提供します。

カスタマ・サクセス・マネージャ: お客様との主な連絡窓口として、お客様がサービスから総合的な価値を得られるよう尽力します。

データソース

ベンダーに依存しないデータ取り込みにより、セキュリティ監視および対応は、テクノロジスタックに関わらず、既存のネットワークおよびセキュリティフレームワークにシームレスに統合できます。これにより、大規模な先行投資の必要性が軽減され、脅威の状況をより包括的に把握できるようになります。サードパーティおよびロックウェル・オートメーションのデータソースには、以下が含まれます。

侵入検知システム – 産業用制御システム、SCADA ネットワーク、その他の重要なインフラを監視して不正アクセスや異常な動作を検出し、運用の中断を回避しながら脅威を検出するように設計されています。

ファイアウォールとDMZ – プロトコル対応フィルタ、定義済みポリシー、安全な中間ゾーンを使用して産業システムと外部ネットワーク間の制御を可能にし、IT-OT 間の直接通信を防ぎながら必要なデータ交換を可能にします。

脆弱性とリスク管理 – 物理プロセスを制御するシステムのセキュリティ上の弱点を特定して対処するとともに、脆弱性を評価して優先順位を付け、効果的な軽減戦略を実装します。

IDと資産の管理 – ユーザIDを確認し、アクセス権限を管理することで、許可されたユーザのみがOTシステムとリソースにアクセスできるようにします。また、すべてのOT資産の正確なインベントリを維持して、構成を追跡し、状態を監視し、脆弱性を特定します。

SOCインフラ

セキュリティ情報イベント管理 (SIEM)

組織のデジタル環境全体からイベントデータを収集、集約、分析し、潜在的なセキュリティ脅威の検出、優先順位付け、対応を支援する一元管理プラットフォーム

セキュリティオーケストレーション、自動化、および対応(SOAR)

ツールを統合し、反復的なタスクを自動化し、システム間でワークフローを調整することで、セキュリティチームがサイバー脅威への対応を合理化し、迅速化できるようにするテクノロジプラットフォームです。

脅威インテリジェンス

現在および新たなサイバー脅威に関する、侵害の兆候、戦術、手法、手順、攻撃者の行動パターンなど、厳選されたコンテキスト情報。これにより、より迅速かつ正確な脅威の検出と対応が可能になります。

報告とチケット発行

透明性、説明責任、継続的な改善を維持するために、セキュリティイベント、アラート、インシデント解決活動を文書化、追跡、伝達する構造化されたプロセス

サイバー脅威は待ってくれません。なぜそうすべきなのでしょうか?

セキュリティ監視と対応がOT環境のセキュリティ確保にどのように役立つか、ぜひ当社までご相談ください。

セキュリティ監視および対応についてご覧ください。

詳細は、**www.rockwellautomation.com**をご覧ください。

Rockwell Automation

expanding **human possibility**®

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846
ロックウェル オートメーション ジャパン株式会社　本社営業部 東京都中央区新川1-3-17新川三幸ビル・中部支店 名古屋市中区錦1-6-5名古屋錦シティビル・関西支店 大阪市淀川区宮原4-1-14住友生命新大阪北ビル・製品に関するお問い合わせ TEL: 03-3206-2784(カスタマケア)

Connect with us.

Publication GMSN-PP013A-JA-P - April 2025