SOLUTION BRIEF

FortiDeceptor によるオペレーショナルテクノロジーのサイバーセキュリティの保証

概要

産業施設のオペレーショナルテクノロジー（OT）のリーダーたちの報告によると、ネットワーク環境の閉じたシステムから開かれたシステムへの移行が進んでいることで、OT システムへの侵入が前年比で 20% も増加しています[1]。この移行により、サイバー攻撃に新たな脅威ベクトルが生まれることになりました。これらの組織の多くは、OT 環境に従来から存在する SCADA（監視制御 / データ取得）や ICS（産業制御システム）のデバイスの保護が十分ではありません。互換性のない IT セキュリティ制御や OT と IT の両方の環境に広がるホリスティックセキュリティインフラストラクチャの構築に伴う複雑さにより、多くの問題が発生しています。

FortiDeceptor は、OT や IT の環境を標的にする脅威の早期検知をシンプルで使いやすい方法で可能にする、ネットワークベースのソリューションです。デコイ（おとり）やハニートークン * を採用して、サイバー攻撃の封じ込めを自動化することで、深刻な被害の発生を防止します。

* ハニーポットの一種

「OT 環境の多くは古くから存在していた孤島のようなものだ。IT ネットワークと相互接続すれば、サイバー攻撃やマルウェアという捕食者を OT 環境に招き入れることになる。」

– 「Securing Operational Technology in Dynamic Landscape」、フォーティネット、Joe Robertson[2]

脆弱な OT 環境の増加

OT ネットワーク環境と IT 環境の統合が進んで外部からのアクセスが可能になっていることで、IT で多く見つかるタイプの侵入に対して脆弱な OT システムが増加しています（図 1 参照）。次のような例が確認されています。

- IT の脅威が OT 環境を標的にする攻撃に再利用される、EKANS ランサムウェアなどの脅威
- OT を専門に標的にする、Stuxnet などの脅威
- IT ネットワークから OT に、またはその反対方向に水平移動する攻撃
- パッチを適用できない古い OT システムを標的にするゼロデイ脅威

OT インフラストラクチャの設計と構築にあたってサイバーセキュリティを考慮しなかった組織は、セキュリティ制御を後で追加して実装する必要があります。さらには、サイバー攻撃による運用中断を減災したり、業界の新しい規制を順守することでコンプライアンス違反による罰則を最小限にしたりする必要もあるでしょう。しかしながら、古いシステム、セキュリティの実装に伴うダウンタイム、IT 向けと OT 向けの異なるセキュリティアプローチの複雑な混在などの理由から、セキュリティの導入が困難になる可能性もあります。

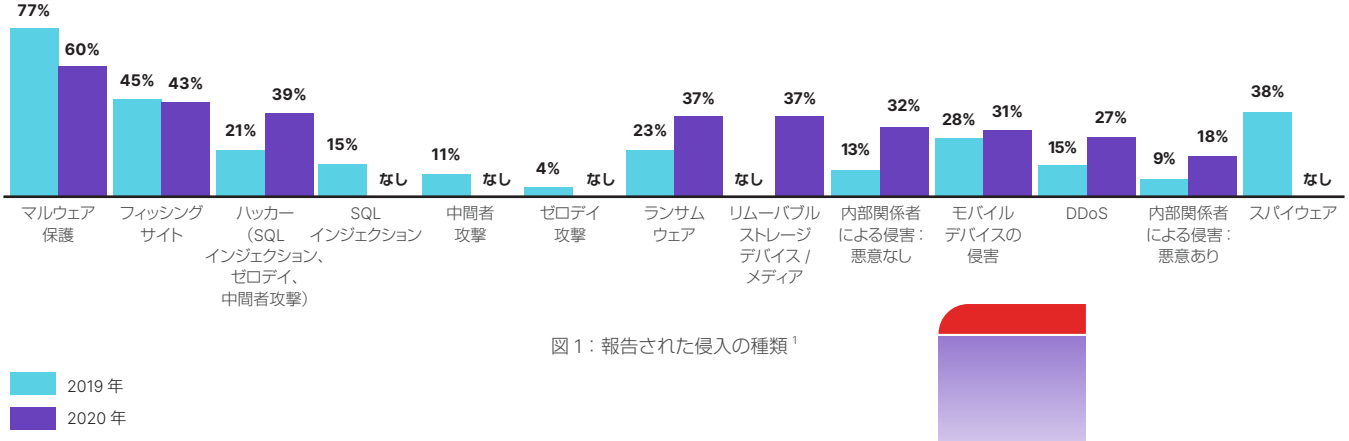

図 1：報告された侵入の種類[1]

IT ベースのセキュリティソリューションの OT への適用を検討することもできますが、これらのソリューションは OT システムを考慮して設計されたものではありません。そのため、次のような問題が発生します。

- 最新のアンチウイルスソフトウェア製品は、OS（オペレーティングシステム）をサポートしていない、ハードウェアの最低要件を満たしていないなどの理由で、多くの場合古いシステムと互換性がない
- 一般的なファイアウォールは、IT ベースのサービスやアプリケーションに含まれる脅威を検知できるが、OPC、BACnet、Modbus などの OT 通信を解読できない
- 一般的な侵入検知や防御のシステムは、IT ベースのアプリケーションの脆弱性の保護は可能だが、OT ベースの脆弱性を保護できない
- ほとんどの外部脅威フィードは、IT には適用できるが、OT には適用できない

FortiDeceptor が導入されている環境の約半数は、エネルギー / 公益事業、運輸、物流などの OT 分野や、化学、食品 / 飲料、自動車、航空宇宙、防衛などの製造分野です。

ネットワーク資産のシミュレーション

サイバーセキュリティの実装にあたってインフラストラクチャを変更したり運用をオフラインにしたりする必要がある他のセキュリティソリューションとは異なり、FortiDeceptor は、使いやすく、既存の環境に影響することはありません。サイバー犯罪者を重要な資産から遠ざけるため、ネットワークや資産をエミュレーションする偽の環境が作成されます。FortiDeceptor は、差し迫った攻撃の早期アラートを生成することで、自動レスポンスによる IT と OT の両方のセグメントの保護を可能にします。

従来のディセプションソリューションは、手動のプロセスでネットワークを分析し、デコイやハニートークンを作成していたため、セットアップが困難でした。FortiDeceptor は、環境内のネットワークや資産を自動的に検出し、AI（人工知能）を活用して、デコイ（おとり）、関連アプリケーションサービス、ネットワーク構成を推奨します。これらの構成の確定後にユーザーが導入を指示するだけで、FortiDeceptor が以降の処理をすべて実行してくれます。分散する FortiDeceptor の導入環境をプライマリノードから一元管理することもできます。

FortiDeceptor では、エージェントのインストールにあたって、SCADA / ICS をオフラインにする必要はありません。FortiDeceptor が、本物の環境をシミュレーションする偽の環境を作成し、ハニーポットの概念を使用して脅威を発見します。デコイやハニートークンのネットワークでの活動を受動的に監視するため、FortiDeceptor による遅延は発生しません。

サイバーキルチェーンの最初の段階では、犯罪者が本格的な攻撃を開始する前の一般的な偵察活動を実行して、環境を理解し、標的になりそうな資産を特定します [3]。FortiDeceptor の偽の環境と本物の環境の区別は不可能であるため、偵察の段階でデコイに接触した直後にアラートが発行されます。従業員がやり取りするのは本物の環境だけであるため、アラートが誤って発行されることはありません。FortiDeceptor は、犯罪者の戦術を捕捉し、環境への侵入方法、目的、使用されたツールなどを明らかにします。

OT と IT を保護する脅威レスポンスオプション

FortiDeceptor は、犯罪者のすべての行動を攻撃のタイムラインに相関付けることで、TTP（戦術、手法、手順）のコンテキスト情報を提供し、新たに発見された脅威を減災するオプションを提供します。大規模のセキュリティオペレーションセンター（SOC）を運用する組織は、ディセプションを活用して犯罪者の行動を調査し、調査の完了後に必要な減災や対策を実行できるでしょう。それ以外の組織も、ディセプションを脅威のレスポンスや追跡をサポートする自らの自動化フレームワークに統合できるでしょう。

FortiDeceptor はフォーティネット セキュリティ ファブリックを構成する要素であるため、以下のフォーティネット製品とのシームレスな統合をサポートします。

- FortiGate：次世代ファイアウォール
- FortiNAC：ネットワークアクセス制御
- FortiSOAR：セキュリティオーケストレーション、自動化、レスポンス
- FortiSIEM：セキュリティ情報 / イベント管理
- FortiAnalyzer：分析型セキュリティ管理

FortiDeceptor はファブリックコネクタを使用することで、サードパーティのセキュリティソリューションとの統合が可能になります。

Rockwell Ethernet / IP や Siemens S7 など、広範な SCADA / ICS サポートを提供しています。Windows や Linux のクライアントやサーバーのシミュレーションにより、組織の IT 部門に幅広く対応します。ディセプションは、デバイスそのもののだけでなく、Git リポジトリ、VPN（仮想プライベートネットワーク）、SMB（サーバーメッセージブロック）、SQL（構造化クエリ言語）などのさまざまなアプリケーションやサービスをサポートしています。

セキュリティの成熟度が高い多くの組織が、NIST や MITRE などのセキュリティフレームワークを採用しています。ICS アーキテクチャの近代化を検討している産業施設は、IT ネットワークにまで広がる OT ネットワークの各ゾーンにセキュリティを適用する体系的アプローチとして、Purdue モデル * を検討することもあるでしょう。FortiDeceptor は、Purdue モデルのプロセス制御、運用および制御、ビジネスおよびエンタープライズなどのさまざまな Purdue ゾーンに適用します。

* Purdueモデル（システムを分割･階層化し、保護する対象を可視化するリファレンス）

FortiDeceptor を導入すべき理由

FortiDeceptor は、強力なセキュリティ、幅広い対応、自動化された保護という 3 つの重要なビジネスメリットを提供します。脅威の発生源であるサイバー犯罪者に焦点を当てているため、組織のセキュリティ戦略にとって強力な付加価値となります。ディセプションの早期の検知とレスポンスの特性をプロアクティブな防御戦略として組み込むことで、既存のセキュリティ態勢を強化し、外部や内部の脅威によるビジネスの混乱を軽減できます。

OT 環境へのセキュリティの導入は複雑ですが、FortiDeceptor は、既存の環境に影響することなく容易に導入でき、導入前、導入時、導入後に OT 運用が遅延することもありません。FortiDeceptor は OT 環境だけではなく、IT にも対応し、動的な攻撃対象領域の包括的な保護を可能にするため、セキュリティ運用担当者は、セキュリティギャップを解消できます。最も重要な点として、FortiDeceptor はフォーティネット セキュリティ ファブリックの一部であるため、フォーティネットやサードパーティのセキュリティソリューションと容易に統合して脅威のレスポンスとコンテキスト（攻撃の挙動や推移）に基づく脅威の追跡を自動化し、SOC プロセスにおける効率性の向上と SecOps のさらなる拡張が可能になります。

[1] 「2020 State of Operational Technology and Cybersecurity Report」、フォーティネット、2020 年 6 月 30 日、（英語）：
https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-state-of-operational-technology.pdf

[2] 「Looking Back and Forward: Critical Takeaways for Operational Technology Security」、Rick Peters 著、フォーティネット、2020 年 12 月 2 日、（英語）：
https://www.fortinet.com/blog/ciso-collective/looking-back-and-forward-critical-takeaways-for-ot-security

[3] 「The Cyber Kill Chain」、Lockheed Martin、2021 年 4 月 28 日、（英語）：https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

SB-OT-FortiDeceptor-202106-R1