CUSTOMER STORY

特殊化学薬品メーカーが IT/OTインフラ全体でセキュリティの継続性を維持

FireEyeのソリューションが人員、プロセス、テクノロジーを活性化

概要

業界

製造

ソリューション

- FireEyeネットワーク・セキュリティ
- FireEyeエンドポイント・セキュリティ
- FireEye Helix
- Mandiant Managed Defense
- Mandiant Threat Intelligence
- FireEye Malware Analysis
- FireEye Security Orchestrator
- Mandiantインシデントレスポンス・リテイナー
- Mandiant侵害調査サービス

利点

- 1つのプロバイダーからセキュリティ・ソリューションを導入し、ハイブリッドな環境下で包括的な保護を実現
- 単一のダッシュボードを使用して、IT/OTトラフィックをまとめた統合モニタリング
- FireEyeが提供する環境データにより、リスク診断とセキュリティ投資のコスト分析を実施
- 直感的な設計のソリューションにより、新規の担当者の習得がスピードアップし、リソース効率が大幅にアップ

企業紹介

このメーカーは、主要産業や消費者物資に使用されるさまざまな製品の原料となる物質を製造しています。米国に本社を置き、生産ネットワークと製造施設は世界中に広がっています。同社はFortune 500に選出された企業です。

わずかなミスが壊滅的な被害につながる製造分野では、従業員、地域コミュニティ、そして環境に対する真摯な取り組みが何より重要になります。特殊化学薬品の大量生産と安全なオペレーションとを両立させるには、従来の事務部門の情報テクノロジー（IT）とオペレーション・テクノロジー（OT）の両方を含む、非常に多くの要素から成るグローバル・インフラが必要になります。このOTには、バルブの制御など工場のオペレーションに必須の産業制御システム（ICS）、プログラマブル論理のコントローラ、SCADAシステムなど、多くのものが含まれます。

メーカーは、ITドメインだけでなく、OT環境のインフラ上に製品が存在しているため、サイバー攻撃の格好の標的となります。同社の最高情報セキュリティ責任者（CISO）は次のように説明しています。「当社では、非常に不安定な物質を工場内で移動させることが多いため、こうした物質の温度や量、圧力の監視と管理を行う制御システムが一部でも侵害されると、大きな被害につながる恐れがあります。最終的には人命にも危害が及びかねません」

このCISOは、IT/OTのハイブリッド環境のサイバー・セキュリティに関する包括的なアプローチには、OTの進化についての認識を深め、ITとの相互接続性を高めることが必要だと考えました。従来、ITセキュリティにはCSOやCISOが重点的に取り組んできましたが、OT機器のセキュリティの責任は、プロセス制御エンジニアとオペレーション設備のメーカーの努力に依存してきました。インフラの統合が進み、クラウドやインターネットに接続されたテクノロジーが登場してくる中で、組織はサイバー・セキュリティのあり方を考え直す時期にきています。

「FireEyeは当初から、実に素晴らしいチームを当社に提供してくれました。私は25年間サイバー・セキュリティに携わっていますが、FireEyeのアカウント・チームはおそらく、これまでに出会った最高のチームです」

— 最高情報セキュリティ責任者、特殊化学薬品メーカー

このメーカーの複雑で多面的な環境に対する強力な防御体制を構築するために、CISOは資産管理の改善に重点を置きました。そして、同社のテクノロジー体制に追加基準を導入し、一貫性を高めることができました。

CISOはまた、IT分野とOT分野の共有経路から生じる脆弱性に対処することが重要だと考えました。「OTスペースで最大の問題の1つが、サードパーティのアクセスでした。当社の工場では、常時15〜20の業者が働いています。これらの業者は当社のインフラに物理的にアクセスしますし、当社のシステムにハードウェアを接続することも可能であり、当社のネットワークに接続しなければならない場合もあります。この状況が、従来のセキュリティ戦略では対処しきれない課題でした。

最適なパッケージ

あらゆるセキュリティ担当の責任者が次のような選択を迫られています。多数の異なるベンダーから個別の製品を選んで自分なりのセキュリティ体制を構築するか、主要なセキュリティ・ソリューション・サプライヤーを選んで統合されたアプローチを取り、複数の攻撃経路にわたる保護を手に入れるかです。このCISOは後者の戦略を選び、最適なプロバイダーを特定するようチームに命じました。

「市場調査の結果、すぐに浮かび上がったのがFireEyeのポートフォリオでした」と彼は回想します。「ソリューションの質の高さに加え、FireEyeは当初から、実に素晴らしいチームを当社に提供してくれました。私は25年間サイバー・セキュリティに携わっていますが、FireEyeのアカウント・チームはおそらく、これまでに出会った最高のチームです」

このメーカーでは、NISTサイバー・セキュリティ・フレームワークと、NISTのNICEサイバー・セキュリティ・ワークフォース・フレームワークを統合したものを導入し、リファレンス・アーキテクチャを最適化する最良の方法を判断しました。CISOは、同社のセキュリティ体制を強化するためには、同社のセキュリティ・オペレーション・センター（SOC）とそれを支える3本柱である、人員、プロセス、テクノロジーを進化させることが必須であると考えるに至りました。

テクノロジーの観点から、同社はFireEye Helixのセキュリティ・オペレーション・プラットフォームに基づく一連のセキュリティ・コンポーネントを導入しました。また、FireEye Malware AnalysisとFireEye Security Orchestratorを使用して、セキュリティ・プロセスを強化しました。徹底的な侵害調査の結果、Mandiant Managed DefenseとMandiantインシデントレスポンス・リテイナー・サービスが追加され、これによって防御力がさらに高まり、チームの人員のスキルと有効性が強化されました。

FireEyeソリューションは、FireEye Helixの単一の統合インターフェイスを使用することでスムーズに連携します。CISOはこう語ります。「FireEyeソリューションは直感的に使えて、1か所からすべてを見渡すことができます。しかも新規の担当者が非常に短期間で学ぶことができるため、若手とベテランが混在している当社のチームには最適です」

国家レベルの攻撃を阻止

Mandiant Managed Defenseは、同社のセキュリティ戦略において必須のアセットとなっています。Managed Defenseアナリストによる24時間体制のサービスのおかげで、同社のSOCが強化され、リソースの最適化が可能になります。チームは単にアラートを追いかけるのではなく、重要な脅威に集中して対処できます。導入以来、Managed Defenseは、国家支援を受けた高度な攻撃から同社のインフラを守り、攻撃から侵害への進展を防いでいます。

IT/OTの連続性のあらゆる面でのセキュリティ能力を拡張するため、FireEyeではICS分野における優れた企業と提携しています。FireEyeとWaterfall Securityとの連携によって、このCISOは同社の広範なOT環境に対するMandiant Managed DefenseとFireEye Helixの保護を拡大しました。彼は次のように語っています。「WaterfallのUnidirectional CloudConnectゲートウェイによって、FireEyeのポートフォリオのあらゆる利点を産業制御インフラにも適用し、OT環境からデータを収集できるようになりました。IT分野と同じように、当社のSIEMがこのOTトラフィックを調べ、不審な活動を特定して阻止できるのです」

「取締役会で防御戦略について話し合っているとき、『FireEye』という言葉を出すだけで、緊張がほぐれ、役員が安心するのがわかります。このことがすべてを物語っています」

— 最高情報セキュリティ責任者、特殊化学薬品メーカー

測定できれば、改善できる

統合されたIT/OT環境から取得したデータの解析は、このメーカーがサイバー・セキュリティ体制の有効性を示す基準を得るうえで重要な役目を果たしています。「当社では、脅威に対する露出度と脆弱性の詳細情報を示すSOCのデータをFireEyeソリューションから得て、そのデータに照らして各装置の年間の収益評価を行うという、OT分野専用のリスク管理メカニズムを構築しました。この結果として得られるリスク・スコアは、セキュリティ・インフラへの投資により達成した利益を経営陣が理解するために役立っています」

「また、オンサイトのFireEyeチームが、脆弱性管理プログラムの構成を助けてくれています。たとえば、復元までの平均時間やトリアージまでの平均時間といったKPIの選択に加え、FireEye Threat Intelligenceの情報フィードと脆弱性データを、全体のリスク・スコアに組み入れています」と、CISOは語ります。「FireEyeのデータは、当社にとって非常に重要です。私たちは『測定できれば、改善できる』という格言を信じており、現在私たちが使用しているデータの95%はFireEyeソリューションから来ています」

同社のIT/OTインフラは非常に動的な性質のものですが、FireEyeは、サイバー犯罪者の一歩先を行けるように、同社の組織全体に信頼を構築しています。「取締役会で防御戦略について話し合っているとき、『FireEye』という言葉を出すだけで、緊張がほぐれ、役員が安心するのがわかります。このことがすべてを物語っています」と、CISOは語ります。

企業のDNAに組み込まれたサイバー・セキュリティ

特殊化学薬品メーカーである同社にとって、信頼と安全性は事業の核心です。同社の掲げる目標は、従業員、請負業者、環境、コミュニティのいずれにも危害を与えずに、100%の品質と信頼性を達成することです。

この取り組みの一環として、同社では事業の成功と社会的責任との間のつながりを強化するイニシアチブを進めています。「当社では、企業のDNAにサイバー・セキュリティを組み込み、業務の優先事項に整合させています。サイバー攻撃から身を守るためのアプローチについて、全社にわたってトレーニングと基準を導入し、責任意識を育んでいます」とCISOは強調します。

「FireEyeはかけがえのないパートナーであり、当社のセキュリティ体制を改善するうえで重要な存在です。当社のIT分野のセキュリティ保護を支援し、防御力をOTに拡大するために協力しています」

FireEyeの詳細については、**www.FireEye.jp**をご覧ください。

ファイア・アイ株式会社
〒101-0054 東京都千代田区神田錦町3-22
テラススクエア8階 | 03-4577-4401 |
Japan@fireeye.com

FireEyeについて

FireEyeは、インテリジェンス主導型のセキュリティ企業です。お客様は、FireEyeの革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名なMandiant®コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。このアプローチにより、FireEyeは準備、防御、インシデントレスポンスといった、組織がサイバー攻撃対策をする上での課題となっていた複雑性や負担を解消します。

FIREEYE™