CUSTOMER STORY

国際鉄道オペレーターの ITおよびOTシステムを守る

公共交通ネットワークの保護に役立つ多様なFireEyeポートフォリオ

概要

業界

運輸

ソリューション

- FireEyeネットワーク・セキュリティ（SmartVision）
- FireEyeエンドポイント・セキュリティ
- FireEye Eメール・セキュリティ
- FireEye ICS HealthCheck
- Mandiant Managed Defense
- FireEye Mandiantインシデントレスポンス・リテイナー
- FireEye Mandiantコンサルティング・サービス

利点

- サイバー・セキュリティ・チームの効果と効率を、世界トップレベルのソリューションとサービスで強化
- GDPRやPDPOといった地域特有のデータ・セキュリティ規制へのコンプライアンスを簡素化
- グローバルのインフラ全体にわたる詳細な可視化
- バイアスのない中立的なアドバイスにより、セキュリティ体制全体を強化

企業紹介

この鉄道会社は約半世紀にわたって、完璧な公共交通サービスを提供してきました。数万人の職員が、複数の国で鉄道の運行を管理し、世界中で一日に数百万人の利用客を見守っています。

高い安全性と効率、信頼性で知られるこの公共交通ネットワークは、世界中の多くの都市にとって、最新の鉄道オペレーションの規範となっています。

毎日、何百万人もの人々が、安全に目的地まで通勤、通学するために、同社の鉄道を利用しています。この鉄道会社の人気の理由は、時間の正確さと、テクノロジーで強化された設備にあります。利用者は、携帯電話アプリや自動運賃収集システムといったアメニティを通してシームレスな体験が得られます。

この鉄道会社の最高情報責任者（CIO）の責務は、不正なサイバー活動によるサービスの中断なしに、日常業務がスムーズに運ぶようにすることです。CIOの任務は、同社の機密情報の機密性、完全性、可用性（CIA）を維持することが中心です。

名前の知られた企業であるため、何らかの侵害が生じれば、企業のブランドや顧客の信頼が傷つけられることになります。最悪の場合、何百kmにも及ぶ路線の安全な運行が危険にさらされます。CIOは次のように語っています。「当社にとって、安全は何よりも重要です。極端な話、当社のシステムが侵害されると、顧客の安全にも影響が及ぶ可能性があります」

同社には、ITおよび産業制御システム（ICS）を防御するための確固たるサイバー・セキュリティ体制を維持する責任に加え、1,000万人を超える利用客と従業員の個人情報を保護する責任もあります。さらに、EUのGDPRをはじめとする複数のデータ・セキュリティ関連の規制にも準拠しなければなりません。

「FireEyeは多くの組織にとって信頼の置けるパートナーとなっていますが、当社にとって、そして私個人にとっては、特にそう言えます」

— 最高情報責任者（CIO）、国際鉄道会社

今日、明日、そして遠い未来を見据えた強靭な防御

同社のセキュリティ・チームは、テクノロジー製品の選定にあたって、サイバー・セキュリティの世界的な標準に照らして数々の製品を評価しました。CIOは特に、各ツールのロードマップの理解に重点を置きました。世界的なデジタル・トランスフォーメーションの結果として生じてくる新たな脆弱性やサイバー攻撃の形態に合わせて、変化、対処していけるソリューションを求めたのです。また同社は、セキュリティ・サプライヤーの各地域およびグローバルのサポート・チームについて、その質とアクセス性に注目しました。

厳しい選定プロセスを経て、セキュリティ・チームが選んだのがFireEyeでした。FireEye Mandiantのコンサルタントは、同社のネットワーク・インフラと産業制御システムの全体を診断しました。診断結果と、セキュリティを改善するための推奨事項に基づいて、FireEyeネットワーク・セキュリティ、FireEye Eメール・セキュリティ、FireEyeエンドポイント・セキュリティが導入されました。

セキュリティ・チームはさらに、ネットワーク内の水平展開に対する可視性を高め、不正な活動がネットワークに侵入した後にタイムリーに検知できるよう、FireEyeネットワーク・セキュリティのコンポーネントであるFireEye SmartVisionも環境に導入しました。

FireEyeのこれら全てのテクノロジーが連携し、コアから境界に至るインフラ全体を保護するため、鉄道会社はデータ管理の責任を果たすことができます。このセキュリティ体制は、侵害の検知を自動化し、インシデント対応を簡略化するので、同社は個人データの不正使用を防ぐためのデータ侵害の通知義務と要件に準拠する装備を強化できます。最初の導入が成功したことを受けて、セキュリティ・チームは同じ戦略を他の地域の子会社にも適用しました。

最前線で得られたインテリジェンスを活用

FireEyeのコンサルタントは、世界中で起きている大規模で被害の大きい侵害に最前線で対応しています。その経験から得られた脅威インテリジェンスを惜しみなく共有しました。このコンサルタントの専門知識も、FireEyeを選定する際の決め手となりました。「サイバー・セキュリティは常に変化しています。この課題に対処するために必要な人材を確保することは、どんなに魅力ある一流企業であっても難しいでしょう」と、CIOは説明します。

「FireEye Mandiantのチームから得られる専門的なガイダンスは、実に貴重なものだと思います。FireEyeのソリューションに直接関係のない質問であっても、コンサルタントはバイアスのない中立的なアドバイスをしてくれます」

この鉄道会社はFireEye ICS HealthCheckも導入しました。これは、IT環境とICS環境の両方にわたって、同じ程度に厳しいセキュリティを適用するためです。Mandiantのコンサルタントは、ワークショップによるICSアーキテクチャのレビューを実施し、詳細な技術解析も行いました。

FireEye Mandiantインシデントレスポンス・リテイナー（IRR）も追加され、同社は不正な活動を迅速に特定し、攻撃に関するコンテキスト情報を受け取る機能も手に入れました。これで、サイバー・インシデントにさらに迅速かつ効果的に対応できるようになりました。

信頼できるサイバー・セキュリティ・テクノロジーのパートナーを見つける

FireEyeのソリューションを導入したことにより、CIOはサイバー・セキュリティ攻撃に対する組織の備えに安心感が得られたと言います。「当社にとって一番重要なのは、システムの安全性であり、その提供能力に自信を持ちたいと常に思っています。今では、FireEyeを、特にそのインシデント対応体制を信頼できることがわかっており、かつてない安心感を与えてくれます」と彼は言います。

同社のセキュリティ体制にFireEyeのソリューションが与えた影響について、CIOは次のように締めくくりました。「FireEyeは非常に幅広いソリューションを提供しています。これがさらに、Mandiantのコンサルタントが有する専門知識によって補完されています。FireEyeは多くの組織にとって信頼の置けるパートナーとなっています。当社にとって、そして私個人にとっては、特にそう言えます」

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™