CUSTOMER STORY

大手鉄道会社のネットワークが サイバー・セキュリティの予防的アプローチを導入

鉄道会社がFireEyeソリューションで重要なインフラを防御

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
- FireEyeエンドポイント・セキュリティ
- Mandiant Managed Defense
- FireEye Network Forensics
- Mandiant Security
- Validation Platform

利点

- 強化された可視性と具体的な脅威インテリジェンスにより、セキュリティ対策の予防的なアプローチを実現
- 正確なアラートと質の高いレポートにより、SOCのアラート疲れを軽減
- 24時間体制でリアルタイムで監視し、カスタマイズされたセキュリティ対策を迅速に導入
- FireEyeのテクノロジー、インテリジェンス、専門知識を独自に融合させ、全体的なセキュリティ体制を強化

企業紹介

この米国大手の鉄道運営会社は、農作物、消費者製品、工業製品、石炭を、米国内の数万マイルに及ぶ路線で輸送しています。

この企業は、食料、電力、その他の生活必需品を供給する使命を担い、国の重要インフラの一部として国に指定されています。同社の鉄道は毎年大量の貨物を運搬し、高速道路の混雑の緩和や、道路車両による二酸化炭素放出量の低減に大きく貢献しています。

複数のグローバル・サプライ・チェーンの重要な構成要素であり、何百万人ものアメリカ市民の経済と日常生活に欠かせない存在として、同社のインフラにはサイバー攻撃に対する効果的な保護が必要です。この鉄道のセキュリティ・オペレーション・センター（SOC）のマネージャーは次のように語っています。「私たちは膨大な量の商品を全国に輸送しており、それが米国において当社に成功をもたらしています。当社が標的にされるような地政学的な出来事に対して、警戒を怠らないことが重要だと考えています」

SOCでは、同社のITオペレーションや鉄道インフラを標的とするあらゆるサイバー脅威を管理しています。SOCのマネージャーとそのチームは、24時間体制でアラートの分析、脅威への対応、インシデント対応を行っています。SOCの働きによって、何千もの顧客アカウントの濫用を防ぎ、膨大な数のメール・アカウントの悪用を妨げ、同社の広範なエンドポイントをサイバー攻撃から守っています。

「当社は、最新の脅威に最前線で立ち向かうチームに守られ、当社の環境の保護に投資しています。FireEyeは私たち同様、当社のことを米国にとって非常に重要な存在だと考えてくれています」

— SOCマネージャー、米国の大手鉄道会社

この鉄道会社はこれまでも常に厳しいセキュリティ体制をとってきましたが、サイバー攻撃に対して、より効率的で予防的なアプローチを導入したいと考えました。SOCマネージャーはこう説明しています。「私たちは非常に受身的な体制でした。当社のセキュリティ・データはすべて、外から持ち込まれたものでした。フィッシング攻撃が起こっても、ずっと後になってから気づけるかどうかといった具合でした。この運用状況と体制を変えて、被害が生じる前に脅威を特定できるようにしたいと考えたのです」

多ければいいというものではない

この鉄道会社は、SOCのアラート疲れを軽減したいとも考えていました。膨大な数の過検知と莫大な情報量が原因で、正確さや効率性が損なわれ始めていたからです。環境全体にわたって複数のエージェントが使用されており、ばらばらで一貫性のない大量のデータが生成されることから、防御に関わる状況はさらに複雑になっていました。

このマネージャーは特に、鉄道のセキュリティ・ツールとレポート機能の有効性検証に取り組みました。会社が利用するサービスがきちんと機能しているか、手順に従ってSOCが脅威を捕捉し、攻撃の軌跡を正確に特定できるかを診断したいと考えました。

リアルタイムの脅威調査とセキュリティ・インフラ診断

この鉄道会社はまず、FireEyeネットワーク・セキュリティを導入し、環境境界の一部のデバイスにFireEyeエンドポイント・セキュリティを導入しました。さらに、FireEye Network ForensicsとMandiant Managed Defenseのサービスを追加して、SOCの能力を強化しました。

鉄道会社のエッジ・インフラで起きた1件の侵害をSOCチームが見つけたことで、FireEyeソリューションの価値が示されました。FireEyeネットワーク・セキュリティのWeb Shell検知機能を活用することで、SOCチームは不正なスクリプトが同社のサーバーにアップロードされようとしているのを発見したのです。

「その後、FireEyeエンドポイント・セキュリティを使用した調査によって、侵害されたサーバー上で脅威に対処しました。FireEyeの統合ソリューションから得られたインテリジェンスのおかげで、セキュリティ・チームがマッピングを行い、攻撃に対処できました」と、マネージャーは語ります。「FireEye製品によって、標的となったサーバーが特定されました。マルウェアは実際に侵入していましたが、Web Shellがインストールを検証する前に攻撃を止めることができました」

マネージャーはこの解析と対応の成功を機に、SOCの能力を高めて環境全体を監視し、脅威を回避することの利点を会社に伝えました。その結果、FireEyeエンドポイント・セキュリティの導入を拡大することが決まり、FireEyeのソリューションを組み合わせることによって警戒体制が強化されました。

マネージャーは、Mandiant Security Validation PlatformもSOCに導入し、防御の有効性を測定、改善する能力を最適化しました。彼はこう語ります。「ペネトレーション・テストの結果に基づいて対処をしていては、それまでに状況が変わってしまい、変更の効果が薄れてしまいます。Mandiant Security Validation Platformを導入したことで、潜在的なセキュリティ脆弱性を特定し、防御体制の質をほぼリアルタイムで評価できるようになりました」

この鉄道会社は、Mandiant Security Validation Platformから得たデータと、他のFireEyeソリューションから得たインテリジェンスとを組み合わせて、特定のAPTグループや攻撃グループのインジケーターを監視し、攻撃に備えています。「Mandiant Security Validation Platformは、私たちが長い間、セキュリティ業界に対処を求めてきた穴を埋めてくれました」と、マネージャーは述べています。

脅威を軽減するための予防的なアプローチ

この鉄道会社では、膨大な鉄道インフラの安全を守るため、さまざまなソリューション、ツール、サービスをSOCに導入しています。「FireEye製品は業界で信頼を得ているリソースだと、私たちは見ています。当社の脅威ハンティング担当者は、どこよりもFireEyeを頼りにしています」と、マネージャーは明かしてくれました。

「Mandiant Security Validationは、私たちが長い間、セキュリティ業界に対処を求めてきた穴を埋めてくれました」

— SOCマネージャー、米国の大手鉄道会社

この鉄道会社のインフラとSOCの構成は非常に複雑であるにもかかわらず、FireEyeによる質の高いアラートとサポートによって、全体的なセキュリティ体制を簡略化できました。「FireEyeの通知は正確なので、アラート疲れを最小限に抑えることができています。アラートが発生すると、私たちは自社のアナリストに問題の調査に当たってもらうだけでなく、必要に応じてMandiant Managed Defenseチームからの支援も即座に受けることができます」と、セキュリティ担当者は語ります。

質の良いアラート、コアから境界に至る可視性、具体的なインテリジェンスの確かな供給、強力なフォレンジック分析能力を備えたことで、この鉄道会社はサイバー・セキュリティ体制を劇的に改善できました。マネージャーはこう語ります。「不自然な振る舞いを検知したり不審な活動の増加を観察したりしても、私たちは即座にその状況を調査し、その脅威からの潜在的な影響を回避するために適切な戦略を講じることができます」

FireEyeのチームメンバーへの容易なアクセス、サイバー・セキュリティに関するFireEyeの専門知識、そして鉄道固有のセキュリティ体制に関する深い理解は、FireEyeのソリューションとサービスに投資したこの鉄道会社にとって、大きな付加価値となりました。「FireEyeとのやり取りの中で関係する方たちは、私たちにとって重要なカギとなっています。話しやすいことに加え、非常に知識が豊富です」と、マネージャーは強調します。「当社は、最新の脅威に最前線で立ち向かうチームに守られ、当社の環境の保護に投資しています。FireEyeは私たち同様、当社のことを米国にとって非常に重要な存在だと考えてくれています」

パートナーシップの重要性

この鉄道会社とFireEyeとの関係について、SOCマネージャーは次のようにまとめています。「サイバー・セキュリティの分野で私がひとつ学んだことは、インテリジェンスが多すぎるとその中で溺れてしまうということです。インテリジェンスを提供する業者は数多くありますが、世界で何が起きているかを深く理解している業者は多くありません。FireEyeには、マルウェアが生まれる地政学的コンテキストを理解し、解説してくれるアナリストたちがいます。このような詳細情報が今以上に意味を持つようになり、脅威トレンドが急速に進化していく中、当社とFireEyeとの関係はいっそう重要なものになります」

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™