

CUSTOMER STORY

著名な総合医療センターが 防御の範囲を拡大して効率を改善

ペンシルバニア州大学ミルトンS. ハーシー病院 (Penn State Health Milton S. Hershey Medical Center) が FireEye の統合ソリューションとインテリジェンスを活用



概要

業界



医療

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 Eメール・セキュリティ
- FireEye Central Management
- Mandiant Managed Defense

利点

- SOC機能をシームレスに拡大
- 攻撃や脅威の経路全体に対する統合された保護を実施
- セキュリティ体制全体を単一のコンソールで管理

企業紹介

ペンシルバニア州大学ミルトンS. ハーシー病院 (Penn State Health Milton S. Hershey Medical Center) は、ペンシルバニア州ハーシーにある、研究、治療、医療分野でのキャリアを求める学生の育成に注力する機関として有名です。ハーシー病院は、病床550、3千人以上の医療のプロフェッショナルを抱える医療機関であり、毎年3万人の患者を受け入れ、100万人の治療をしています。



ペンシルバニア州大学ミルトンS. ハーシー病院は著名な大学付属病院であり、最先端の医療研究における最高レベルの研究者を数多く抱えています。生涯のキャリアの中で、1つの病気や1つの医療機器のみに取り組む研究者は珍しくありません。ハーシー病院の最高情報セキュリティ責任者であるマシュー・スナイダー (Matthew Snyder) 氏は次のように語ります。「たった1つのデータが侵害されただけで、研究者が20年、30年かけて築いてきた成果が無に帰することもあります。当院にとってサイバー・セキュリティが不可欠かつ重要事項である理由は数多くあり、これはその1つにすぎません」

医療業界が直面するサイバー・セキュリティの課題

医療業界が一年間に受けるサイバー関連の侵害件数は3桁増に上ると、複数の情報源が伝えています。わずか10か月間の期間に、ハーシー病院のインフラに侵入しようとした不正な活動が8,300万件も検知されています。スナイダー氏は次のように語ります。「日常的な偵察活動だけではありません。具体的な侵害活動を試みる攻撃も見つかっています」

統合ソリューションを求めて

統一された電子医療記録 (EHR) とサイバー・セキュリティの統合ソリューションの開発とを例にとり、スナイダー氏は次のように語ります。「電子医療記録とは、医療機器データ、診断情報、医師のメモといった複数のさまざまな情報源からのデータを同化させ、1つの場所にまとめることです。サイバー防御と脅威インテリジェンスについても、それと同じような機能をもたせたいと私たちは考えました」

「複数のFireEye製品による包括的な機能と直感的に対応できる統合ソリューションにより、当センターは最先端の脅威対策を実施することができます。それに加えて、Mandiant Managed Defenseが重要なサポートの役割を果たしており、Mandiantの専門家たちが、いわば当センターのインシデント対応部門の拡張メンバーとして支援してくれます」

— マシュー・スナイダー氏、最高情報セキュリティ責任者、Penn State Health Milton S. Hershey Medical Center

ハーシー病院は、新しいテクノロジーの評価に際して厳しいプロセスを適用しています。スナイダー氏はこう語ります。「新しいセキュリティ関連ソリューションを購入する前に、それがリスクと価値の観点から見て、現在すでにあるセキュリティ・システムに対してさらなる独自かつ定量評価することができる機能を提供できるかを確認します。サイバー・セキュリティ・チームにより特定のサービスの購入が決まれば、組織化されたオンラインでのPoCを実施して、性能と適合性の両面で厳しいテストを行います。

FireEyeの強み

スナイダー氏のチームは、性能に関するテストに最高スコアで合格したFireEyeの統合ソリューションを導入しました。ここでは、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、FireEye Central Management、Mandiant Managed Defenseが含まれます。

「FireEyeソリューションは互いに通信し合い、一体化したインテリジェンスを共通画面に表示します。これは当センターの電子医療記録と同様であり、私たちにとても非常に重要です」と、スナイダー氏は強調します。

「それに加えて、FireEyeエンドポイント・セキュリティは、単に起きたことを知らせるだけでなく、攻撃の前後に起きたことを即座に示してくれます。これは、各アラートに対し、非常に貴重なインテリジェンスとコンテキストをもたらしてくれます。そのため、実際にインシデントが発生した時間における特定のネットワーク・トラフィックを確認したり、攻撃シナリオを再生したりできるのです。必要だと判断された場合は、Mandiant Managed Defenseによる詳細なフォレンジック調査を行います」

Mandiant Managed Defenseは24時間体制で、ハーシー病院のセキュリティ・チームの拡張メンバーとして稼働します。スナイダー氏はこう述べています。「単にアラートを提示するだけのマネージド・セキュリティ・サービス・プロバイダーは望んでいませんでした。Mandiant Managed Defenseを選んだ理由は、質の高いレポートに加え、高精度の検知、調査、ハンティングも提供してくれるからです。Mandiantの専門家は、当センターが有している機能を強化、補完し、私たちがオフラインの時間帯にも監視を続けてくれます」

彼は次のように続けます。「Mandiant Managed Defenseからの侵害レポートには、インシデント対応担当者が実施したステップ・バイ・ステップの貴重な行動項目と、結論の背景となる根拠の説明が含まれています。当センターのインシデント対応チームは、この情報に従って内部で復旧措置を行うことにより、アラートに関係する脅威と、潜在的な脆弱性を除去することができます。Mandiant Managed Defenseのレポートがタイムリーであるという点は非常に重要です。そのおかげで、ほぼリアルタイムでリスクを回避できるからです」

費用対効果の高さと革新性

ハーシー病院では、Mandiant Managed Defenseの費用対効果を高く評価しています。スナイダー氏はこう見積もっています。「セキュリティ・オペレーション・センターを設置すると、新たに12~15人の専任スタッフが必要になる場所でした。Mandiant Managed Defenseのおかげで、はるかに少ない費用で同等もしくはさらに優れた防御ができるようになります」

FireEyeは、ハーシー病院にとって戦略的パートナーとなっています。「複数のFireEye製品による包括的な機能と直感的に対応できる統合ソリューションにより、当センターは最先端の脅威対策を実施することができます。それに加えて、Mandiant Managed Defenseが重要なサポートの役割を果たしており、Mandiantの専門家たちが、いわば当センターのインシデント対応部門の拡張メンバーとして支援してくれます」と、スナイダー氏は語ります。

スナイダー氏はこうまとめています。「FireEyeとのパートナーシップによって、当院には信頼性が生まれました。自身のセンター内のネットワークの侵害インジケーターだけでなく、FireEyeが世界中のインテリジェンス・プラットフォームから得た脅威インテリジェンスも組み合わせることができます。これにより、世界のどこかで起こっている攻撃についても知ることができ、その侵害インジケーターの内容や、そのリスクへの対処法も知ることができます。FireEyeの脅威インテリジェンスは、当センターにとって、侵害の検知、予防、対応のために欠かせない役割を果たしています」

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

©2019 FireEye, Inc. All rights reserved.
FireEyeはFireEye, Inc.の登録商標です。その他のブランド名、製品またはサービス名はそれぞれその所有者の商標またはサービスマークとして登録されている場合があります。
F-EXT-CS-JA-JP-000162-01

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課題となっていた複雑性や負担を解消します。

