

Enterprise Threat Protector によって Perform Group のセキュリティ対策が大きく進化



“ Akamai と協力することで、インフラストラクチャへの脅威を迅速に隔離し、封じ込め、除去できるようになりました。しかも、労力は軽減され整合性は向上しています。

— Daniel Schatz 氏 (Perform Group, CISO)



セキュリティの管理を強化したい

Daniel Schatz 氏は改善が必要だと考えていました。Perform Group は、エンドポイントのウイルス対策とネットワークベースのセキュリティに莫大な資金を投じてきました。しかし、これらのツールをうまく機能させるためには、Perform Group のすべてのインフラストラクチャにおいて、エンドポイントとネットワークロケーションにツールが適切にインストールされ、稼働していなければなりません。さらに、すべてのユーザーが自分のラップトップやデバイスで最新バージョンのウイルス対策を使用しているとは限りません。これもセキュリティリスクを高める要因となっていました。Schatz 氏はこの問題の解決を望んでいました。

感染の拡大を止めることが必要

多くの脅威は阻止されていましたが、見過ごされることもあり、回復に多大な労力を要していました。1 台のラップトップが感染すれば、そこから他の機器にも感染する可能性があります。1 台ずつ追跡し、修正して再構築しなければならず、セキュリティ担当者はこの作業に数時間を費やすことになります。もちろんユーザーの生産性も低下します。

脅威を迅速に特定し、隔離して除去することが必要でしたが、サイバー犯罪はますます巧妙化し、対応は難しくなる一方でした。マルウェア、ランサムウェア、フィッシングによる攻撃が拡がり、リソースが奪われていきます。深刻なデータ漏えいが生じれば、経済的にも、また規制遵守や企業イメージにも悪影響が生じます。同社は常にこの不安を抱えていました。

Akamai が短期間で効果を発揮

慎重な評価の結果、Schatz 氏は、Akamai の Enterprise Threat Protector を採用。悪意ある DNS リクエストを監視しブロックするために、事前防御型のセキュリティレイヤーとして追加することにしたのです。採用の決め手となったのは、実際の脅威に的を絞る、セキュリティアラートの誤検知を最小限に抑える Akamai 脅威インテリジェンスの質の高さでした。この脅威インテリジェンスは、インターネットの IP トラフィックと DNS トラフィックに対する Akamai 独自の視点に基づいたものです。

さらに、Enterprise Threat Protector は導入、展開がシンプルで分かりやすく、必要な作業は Perform Group の既存の DNS サーバーから Akamai のクラウドプラットフォームに DNS トラフィックを転送するよう変更するだけでした。この変更作業はわずか数時間で完了しました。

セキュリティ対策の改善

効果はすぐに現れました。Schatz 氏のセキュリティチームは、Akamai Enterprise Threat Protector の一目見て分かりやすいダッシュボードで、潜在的なセキュリティ問題を把握できるようになりました。Schatz 氏は、「ついに、自社のすべてのコンピューターが何をしているのか把握し、適切な措置をとることができるようになりました」と述べています。

会社

Perform Group
<http://performgroup.com>
Feltham, UK

業種

スポーツ関連のデジタルコンテンツおよびメディア

ソリューション

Akamai 製品 Enterprise Threat Protector

主な成果

- 脅威の特定、隔離、解決を迅速化
- エンドユーザーの適切なふるまいへの依存度を軽減
- 誤検知を低減

Enterprise Threat Protector によって Perform Group のセキュリティ対策が大きく進化

Perform Group のセキュリティチームは、ほぼリアルタイムにアップデートされる Akamai の脅威インテリジェンスに加え、その他の脅威インテリジェンスソースからも悪質なドメインのリストを即座に取り込むことができます。そのため、既存のリソースを活用しながら、Perform Group のネットワーク全体で素早く脅威をブロックできます。エンドユーザー側では何もしなくても脅威の拡散を阻止できるので、セキュリティ対策の耐障害性が大きく向上しました。見過ごされる脅威が減り、万一見過ごされても途中で阻止できます。

Schatz 氏のグループが当初予測したとおり、Enterprise Threat Protector によって不正トラフィックの検知件数が増えました。しかも、Akamai とパートナーを組む前より、誤検知は減少しています。その結果、本当に危険な脅威に注力できるようになり、古い脅威情報による誤検知のセキュリティ警告に時間を浪費することが減りました。余力が生まれたことで、セキュリティチームは、より価値の高いプロジェクトに取り組むこともできるようになりました。そして、Schatz 氏は興味深いことを発見しました。Enterprise Threat Protector によって未知の仮想通貨マイニングが大量に検知されたのです。

将来の方向性

Enterprise Threat Protector のロードマップに強い関心を持った Schatz 氏のグループは、将来に向けた適切なパートナーとして Akamai をとらえています。現在、Perform Group は Akamai と協力して、機能の追加に取り組んでいます。たとえば、疑わしいドメインをリクエストするエンドポイントのリダイレクトとモニタリングによって、問題解決のさらなる迅速化を目指しています。



世界最大、かつ最も信頼性の高いクラウド・デリバリー・プラットフォームを有する Akamai は、デバイスや場所に関係なく、最高、かつ最もセキュアなデジタル体験をお客様に提供します。Akamai のプラットフォームは、比類のないスケールで展開されており、お客様に優れたパフォーマンスとセキュリティを提供しています。ウェブ/モバイルパフォーマンス、クラウドセキュリティ、エンタープライズアクセス、ビデオデリバリーによって構成される Akamai のソリューションポートフォリオは、優れたカスタマーサービスと 365 日/24 時間体制のモニタリングによって支えられています。グローバルトップの金融機関、e コマース事業者、メディア・エンターテインメント企業、政府機関等が、Akamai を信頼する理由について、<https://www.akamai.com/jp/ja/> または <https://blogs.akamai.com/jp/> および Twitter の @Akamai_jp でご紹介しています。公開日：2018 年 6 月。