Delivery Hero社、Splunk Cloud Platformでセキュリティを一元化

主な課題

世界的な成長を遂げたDelivery Hero社は、セキュリティ運用と監視の範囲を拡大し、可視性を向上させる必要に迫られました。潜在的なセキュリティの問題を迅速に発見して修復し、部門を横断して最新情報を共有するためです。

主な成果

Delivery Hero社のグローバルセキュリティチームは、Splunk Cloud Platformを導入することでハイブリッドかつマルチクラウドの自社IT環境を一元的に把握できるようになりました。インサイトをリアルタイムで取得して、脅威や脆弱性、設定ミスの調査に役立てています。

Delivery Hero

業種：オンラインサービス

ソリューション：セキュリティ、プラットフォーム

機能：SIEM/セキュリティ分析、統合セキュリティ運用、調査とフォレンジック

すべてを監視することで何でも配達

Delivery Hero社は、欧州、アジア、ラテンアメリカの70カ国で、オンラインデリバリーサービスの事業を展開し、「最高のエクスペリエンスを迅速かつ手軽に玄関までお届けする」というミッションを掲げています。日々、このミッションを遂行するためには、グローバルに展開するWebサイトサービスの使いやすさと信頼性を維持する必要があります。

しかし、オンプレミスのインフラが妨げとなり、セキュリティチームは複雑なハイブリッド環境全体のセキュリティを包括的に可視化できていませんでした。セキュリティの監視と可視化のために、IT環境全体の異常や設定ミスを速やかに発見して解決できる、一元的な手段が必要でした。

データ活用の成果

- 250以上のアカウントから一元的に監視して時間を節約
- 複雑なマルチクラウド環境全体で遅延を低減
- 14,000を超えるEDRエンドポイントの脅威を検出

遅延の低減と可視性の向上によりアクションまでの時間を短縮

Splunkソリューションを導入したDelivery Hero社では、かつてない速さでセキュリティの脅威やパフォーマンスの問題を発見して解決できるようになりました。セキュリティチームはSplunk Cloud Platformを利用してデータの調査、監視、分析を行い、行動につなげています。異常なアクティビティの検出能力も大幅に向上しました。

Splunk Cloud Platformでは以前のオンプレミス環境よりも遅延が低減したため、グローバルセキュリティチームはより正確な最新の状況を把握できるようになりました。Delivery Hero社の情報セキュリティディレクターを務めるMauro Papa氏は「Splunkをオンプレミスで使用していた頃は、1カ所で集中管理していました。この方法だと、世界各地のチームでそれぞれの所在地に応じた遅延が起きていたはずです」と述べています。

可視性の向上は、アクションまでの時間の短縮という効果を生んでいます。複数のクラウドプロバイダーを利用しオンプレミスのインフラも抱えるDelivery Hero社では、環境の管理が非常に複雑です。それでも、すべてのログをSplunk Cloud Platformに集約したことで、セキュリティチームはクラウド環境内の設定ミスを簡単に検出、特定できるようになりました。さらにSplunkでこれらのデータを相関付け、問題のあるアマゾン ウェブ サービス(AWS)またはGoogle Cloud Platform (GCP)のオーナーにトリガーを送信することで、早期の解決が可能になりました。Papa氏は「以前はオンプレミスのログにのみSplunkを使用していましたから、検出できない設定ミスがありました。現在ではマルチクラウド環境全体にSplunkを使用しています。可視化の範囲が広がり、問題を数分で修復できるようになりました。以前は見逃していた多くの異常を検出できています」と述べています。

レポートをカスタマイズして時間を短縮し職務を遂行

Splunk Cloud Platformで一元的に管理することで、データソースが増えてもセキュリティチームのリソースを無駄に占有することなく対応できるようになりました。例えば、カスタマイズした合理的なアラートシステムにより、不要なアラートやトラブルシューティングに費やす時間が削減されました。「Splunkでアラートをカスタマイズできたので、誤検知率が下がりました」とPapa氏は述べています。

検出と通知だけでなく、関係者に包括的なメトリクスとレポートを提供する際にもSplunkのプラットフォームが役立っています。Splunk Cloud Platformでは、レポートをリアルタイムで作成したり、任意の間隔で作成するようスケジュールしたり、ダッシュボード内で使用したりできます。「脆弱性をすべて追跡し、それぞれの担当者にレポートを送信できるので、それをもとに担当アプリケーションのパフォーマンスを常に把握しておくことができます」とPapa氏は述べています。

これは、Delivery Hero社のグローバルセキュリティチームが職務を遂行してパフォーマンスを維持するために非常に重要です。「世界各地にさまざまなセキュリティチームがあります。全員が自分の担当するレポートやアラートにアクセスでき、改善できるようにすることが重要なのです」とPapa氏は述べています。

Splunk Cloud Platformのダッシュボードはカスタマイズ可能で使いやすく、セキュリティチームが行う監視プロセスをシンプルにすることができます。また、パフォーマンスデータポイントの接続性を高めるシームレスなプラグインが用意されています。例えば、Splunkはプロジェクト管理ツールのJiraとも統合できるため、KPIの追跡や測定が可能です。

> 以前はオンプレミスのログにのみSplunkを使用していましたから、検出できない設定ミスがありました。現在ではクラウド環境全体にSplunk Cloud Platformを使用しています。可視化の範囲が広がり、問題を数分で修復できるようになりました。以前は見逃していた多くの異常を検出できています”
>
> Delivery Hero社
> 情報セキュリティディレクター、
> **Mauro Papa氏**

> Splunk Cloud Platformのおかげで、セキュリティチームがインフラ保守ではなくセキュリティに集中できるようになりました。今、当社のエンジニアたちは、新しいインデックスを構成したり、新しいダッシュボードからインサイトを取得したり、新しい検出機能を設けたりすることに注力しています”
>
> Delivery Hero社
> 情報セキュリティディレクター、
> **Mauro Papa氏**

重要な脅威に集中

Splunk Cloud Platformにより、Delivery Hero社のセキュリティ担当者は時間のかかるインフラの保守作業をする必要がなくなり、今ではパフォーマンスの最適化に集中できています。

Papa氏は次のように述べています。「Splunk Cloud Platformのおかげで、セキュリティチームがインフラ保守ではなくセキュリティに集中できるようになりました。今、当社のセキュリティエンジニアたちは、新しいインデックスを構成したり、新しいダッシュボードからインサイトを取得したり、新しい検出機能を設けたりすることに注力しています」

世界的な成長と足並みを揃えるため、Delivery Hero社のセキュリティチームは次のステップとしてSplunk Enterprise Securityを導入し、データに基づくインサイトの取得を大規模に実現しようとしています。このインサイトは、お客様に「何でも配達」するというDelivery Hero社のミッション遂行に役立てられることでしょう。4大陸の70カ国にまたがるDelivery Hero社のエコシステムは今後も成長し続けます。Delivery Hero社がエコシステムの重要な役割を管理し続けるのをSplunkは強固なパートナーシップで支援します。

営業へのお問い合わせはこちら：https://www.splunk.com/ja_jp/talk-to-sales.html
〒100-0004 千代田区大手町1-1-1 大手町パークビルディング 8階
www.splunk.com/ja_jp
splunkjp@splunk.com

22-26065-Splunk-Delivery Hero-CS2-A4-JA-202302