sysdig | BIGCOMMERCE

CUSTOMER STORY

BigCommerce社、リアルタイムのクラウドセキュリティを実現

BigCommerce社は、あらゆる規模の企業がオンラインストアを簡単に作成、立ち上げ、成長させることができるクラウドベースのeコマースプラットフォームです。同プラットフォームは、使いやすさ、柔軟性、拡張性、そして強固なパートナーエコシステムで知られています。しかし、それだけでなく、BigCommerce社が、セキュリティアップデート、パッチの提供、そしてコンプライアンス規制への対応を顧客のために維持しているという事実が、BigCommerceを特別なものにしています。

2009年に設立されたBigCommerce社は、このユニークなアプローチにより、飛躍的な成長を遂げ、世界中の数万社と取引を行っています。それと同時に、同社は、IT、セキュリティ、エンジニアリングの各チームを無駄なくかつ効率的に運営しています。

BIGCOMMERCE

業種

ソフトウェアテクノロジー

導入前の課題

- 包括的なエンドツーエンドのプラットフォームサポートにより、アドレスの可視性のギャップを解消
- 設定ミスや脆弱性を特定した上で、それらに優先順位　付け　コンプライアンス要件とセキュリティ制御の統一
- できるだけ少ないクリック数で、きめ細かく実用的なインサイトを迅速に生成

導入効果

- 2秒で脅威に対応
- 脆弱性ノイズを80%削減
- 設定ミスや脆弱性の特定と優先順位付けを20%向上

導入前の課題

すべてのCNAPPベンダーは同じではない

BigCommerce社にとって、セキュリティとコンプライアンスは譲れないものです。BigCommerceを利用している小売業者は毎年数10億ドルもの売上を上げており、金銭を目的としてそのような小売業者を狙う脅威アクターが後を絶ちません。BigCommerceの顧客がセキュリティについて1秒たりとも心配する必要がないように、同社では、堅牢なセキュリティスタックを維持してきました。これには、有名なサイバーセキュリティベンダーの提供するクラウドネイティブアプリケーション保護プラットフォーム（CNAPP）が含まれていました。

しかし、残念ながら、BigCommerce社は、このツールの運用が難しいことに気付きました。同ツールがもたらすアラートノイズは実現可能なレベルを超える量のリソースを必要としており、しかも同ツールのベンダーが提供するサポートは、BigCommerce社を不安にさせるものでした。

BigCommerce社のシニアインフラストラクチャーセキュリティエンジニアであるJordan Bodily氏は、次のように語っています。「2つのアップデートの期間中に、このベンダーはランダムにポリシーをプッシュしており、この結果、当社が設定したすべてのポリシーがリセットされ再度トリガされることになりました。また、当社は、特定の数のエージェントに対する導入が行えなかったため、個別にアップデートするか、それともすべてを一度に実行するかを選ばなければなりませんでした」。

そのベンダーとの関係は限界に達していました。Bodily氏と彼のチームは、必要なものを定義することから代替案を探し始めました。

Bodily氏は次のように話しています。「脅威の検知、特にコマンドライン入力をリアルタイムでキャプチャできることが、当社にとって最も重要でした。また、当社は、強力なクラウドセキュリティポスチャー管理（CSPM）コンポーネントと、ランタイム保護を備えたソリューションも必要としていました。これは、自社環境において過剰な権限を与えられている対象を特定できるようにするためです。そのような対象の例としては、クロスアカウント型のリレーションシップを含んでいるバケットや、閉じておく必要のあるオープンポートなどが挙げられます。

また、NIST、PCI、ISO、CISなどのフレームワークに対する継続的なベンチマークを実行する能力も必須要件でした。これにより、BigCommerce社は、リスクと脅威管理の取り組みについて定期的な評価を行えるようになります。さらに、BigCommerce社は、TerraFormに関する完全な統合サポートと共に、セキュリティイベント管理（SIEM）ツールにログを送信する機能を必要としていました。

> 「私たちは、Sysdigが本番環境で使用されているものに関する知識を利用している点が気に入っています。これにより、より適切な情報に基づいたポスチャーに関する決断が行えます。Sysdigは80%以上のノイズを除去できます。要するに、CSPMはSysdigの主力製品であり、それは当社に自信を与えてくれます」。
>
> **Jordan Bodily氏**
> BigCommerce社、シニアインフラストラクチャー
> セキュリティエンジニア

導入効果

検討に値するCNAPPは2つだけだった

BigCommerce社は、長大なベンダーのリストの中から適切なものを探し始めましたが、同社はすぐにベンダーを絞り込むことできました。

Bodily氏は次のように話します。「私たちは、ほとんどのベンダーを排除しました。なぜなら、そのようなベンダーはイベントを集約するので、私たちが情報にアクセスできるようになるまでに時間がかかるからです。スキャン結果を出すのに30分から数時間かかるところがほとんどでした。そのようなソリューションは、当社にとっては役に立ちませんでした」。結果として、BigCommerce社は、Sysdig社ともう1社にベンダーを絞り込みました。

Bodily氏は次のように話します。「その後、当社では、両方のソリューションに何ができるかをさらに詳しく調べました。そして数週間後、Sysdigを導入しました」。

Sysdigを使うことで、セキュリティチームとエンジニアリングチームは、リアルタイムで脆弱性、脅威、設定ミスを特定し、排除できるようになります。また、ランタイムインサイトを活用することにより、脅威データを視覚化し分析するための直感的な方法を確保できます。さらに、Sysdigを利用することで、BigCommerce社は、自らが抱えるコンプライアンス要件を満たすことも可能となります。

> 「私たちは、危険なIPアドレスへのインバウンド接続やアウトバウンド接続が行われていないか、あるいは異常なプロセスが進行していないかどうかを知りたいのです。BigCommerceはeコマースプラットフォームとして、チェックアウトフローもサポートしています。私たちは、プラットフォームに流入するトラフィックと流出するトラフィックを把握したいのです。Sysdigを使えばそれが可能となります」。
>
> **Jordan Bodily氏**
> BigCommerce社、シニアインフラストラクチャー
> セキュリティエンジニア

導入効果

真のリスクをリアルタイムで特定し、優先順位を付ける

Bodily氏は次のように述べています。「私たちは、イベントやログを取得するたびに、ユーザーインターフェイス（UI）を何度もクリックすることなく、それらに可能な限り多くのストーリーを語らせたいのです。そのためには、相互関連付けとコンテキストが不可欠です。SysdigのUIを見れば、何が起きているのかをすぐに知ることができます。これは非常に重要な機能なのです」。

Bodily氏は次のように話します。「私たちは、インバウンド接続や危険なIPアドレスへのアウトバウンド接続が行われていないか、あるいは異常なプロセスが進行していないかどうかを知りたいのです。BigCommerceはeコマースプラットフォームとして、チェックアウトフローもサポートしています。私たちは、プラットフォームに流入するトラフィックと流出するトラフィックを把握したいのです。Sysdigを使えばそれが可能となります」。

また、BigCommerce社は、Sysdigが動作するスピードも高く評価しています。Bodily氏と彼のチームによれば、攻撃者に1時間も先を越されるようなソリューションを利用することは想像もできないとのことです。Bodily氏は次のように話しています。「私は、誰かが当社の環境に侵入していることを、最初の侵入から15分後や数時間後に知りたくはないのです。一方、Sysdigを使えば、潜在的な脅威をリアルタイムで特定した上で、それに対処することができます」。

1秒1秒を大切に

『**2023年度クラウドネイティブセキュリティおよび利用状況レポート**』によれば、クラウドの攻撃者は迅速かつ場当たり的であり、攻撃を仕掛けるのに費やす時間はわずか10分だと言われています。これは、オンプレミス環境での攻撃に費やされる16日と比べると、非常に短い時間となっています。

もう1つの大きなメリットとして、Sysdigが、複数のスキャン間の差分を自動的に生成することが挙げられます。

Bodily氏は次のように話しています。「多くのベンダーのソリューションは差分を提供していません。差分を手作業で処理するのには、非常に多くの時間がかかります。2週間ごとに脆弱性管理を行わなければならない者として、私は、Sysdigを通じて多くの時間を節約できることに、非常に感謝しています」。

「私たちは、Sysdigが本番環境で使用されているものに関する知識を利用している点が気に入っています。これにより、より適切な情報に基づいたポスチャー決定が行えるようになるからです。Sysdigは80%以上のノイズを除去できます。要するに、CSPMはSysdigの主力製品であり、それは当社に自信を与えてくれます」。

導入効果

脆弱性管理に半日を費やす必要はない

Bodily氏は次のように話しています。「Sysdigの導入により可能となった最先端の機能として、SIEMにイベントをフィードすると、それらのイベントに基づいてクエリを構築できることが挙げられます。たとえば、誰かが構成管理ツールであるPuppetの外部にパケットやRubyGemsをインストールしたとします。すると、私たちは実際にアラートを受け取り、すぐにそのインストールを行ったユーザーに連絡を取ることができるのです」。

信じられないかもしれませんが、これはBigCommerceが考えているSysdig活用計画のほんの一部に過ぎません。同社は、PCI 4.0、侵入検知システム、自動化のためにSysdigを活用することも予定しています。

Bodily氏は次のように話しています。「私たちは、脆弱性管理のような手作業のプロセスをできる限り自動化したいと考えています。現在、私たちは脆弱性管理に半日以上を費やすこともあります。Sysdigを使うことで、そのような時間の95%を取り戻せると、つまりそれを10分か15分に短縮できると考えています」。

「最終的な目標は、手作業のほとんどをSysdigに任せて、1人の担当者がその結果を確認できるようにすることです。これにより、私たちは、それ以外のより重要な業務に取り組むことが可能となります」とBodily氏は話しています。

> 「現在、私たちは脆弱性管理に半日以上を費やすこともあります。Sysdigを使うことで、私たちは、そのような時間の95%を取り戻せると、つまりそれを10分か15分に短縮できると考えています」。
>
> **Jordan Bodily氏**
> BigCommerce社、シニアインフラストラクチャー
> セキュリティエンジニア

ベンダーからパートナーへ

BigCommerce社にとってSysdigの持つ最も大きな魅力は、Sysdigのサポート体制でしょう。Bodily氏と彼のチームは、Sysdig社では、製品、エンジニアリング、サポート、そしてセキュリティエンジニアリングというすべての部門が、販売と導入のプロセスに関与していることを目の当たりにして感動しました。また、さらに重要なこととして、製品に関するフィードバックを提供する際に、Sysdigが熱心に耳を傾けてくれたことを高く評価しています。

BigCommerce社のサイバーセキュリティ担当バイスプレジデントであるDan Holden氏は次のように述べています。「私たちが質問をするたびに、SysdigはSlack経由で即日サポートを提供してくれます。これはSysdigが持つ大きな強みであり、最終的に大きな差別化要因となるものです。Sysdigは、非常に面倒見の良い会社です」。

BigCommerce社の詳細は、**bigcommerce.com**をご覧ください。

業種

ソフトウェアテクノロジー

インフラ基盤

Google Cloud Platform (GCP), Amazon Web Services (AWS)

オーケストレーション

Nomad

ソリューション

Sysdig Secure

Sysdigについて

クラウド環境では、1秒1秒が重要となります。攻撃は驚くほどの速さで進行するため、セキュリティチームはビジネスを減速させることなく、攻撃から守る必要があります。Sysdigは、ランタイムインサイトとオープンソースのFalcoを利用することで、リスクにおける変化を即座に検知し、クラウド攻撃をリアルタイムで阻止します。Sysdigは、クラウドのワークロード、アイデンティティ、サービス全体におけるシグナルを相互に関連付けることで、隠れた攻撃経路を明らかにすると共に、真のリスクに優先順位を付けます。予防から防御に至るまで、Sysdigは企業がイノベーションという最重要事項に集中できるよう支援します。詳細は、**sysdig.jp**をご覧ください。

Sysdig. Secure Every Second.

詳細は、**Sysdig.jp**をご覧ください。

デモを依頼 →

sysdig

CUSTOMER STORY