メディアドゥ、電子書籍をはじめとしたデジタルコンテンツ保護に関わる情報の可視化にSplunk Cloud Platformを採用、全社的なリスク管理の一環としてITガバナンスの強化を推進

課題

事業継続に影響を与えうるリスクの1つとしてデジタルコンテンツの情報漏えいに備えるため、各種セキュリティツールのログを統合的に管理し、デジタルコンテンツをいつ誰がどこで何を出し入れしたのかを横断的に把握できる環境整備が課題に。

導入効果

SPL言語を活用することでクエリ処理が柔軟で、第三者機関の評価が高いSplunk Cloud Platformを採用。デジタルコンテンツの動きが可視化できるようになったほか、社員が出版社とデジタルコンテンツをやり取りする際に用いるツールのログ追跡範囲が拡大。ファイル流出の調査も大幅な工数削減に。

Media Do

業種・業界: 情報通信・出版業界

ソリューション: セキュリティプラットフォーム

情報の流れを可視化し、デジタルコンテンツ保護の強化に貢献するSplunk Cloud Platform

「著作物の健全なる創造サイクルの実現」をミッションに掲げ、2,200を超える出版社と150店以上の電子書店の間での電子書籍の流通を支援する電子書籍流通事業で国内No.1の流通シェアを持つ株式会社メディアドゥ。また、IP発掘・創出や電子書籍に関わるあらゆるサービスの提供など様々な事業を展開しており、出版業界における取次というポジションとともに、長年のノウハウや最先端技術を活かして、コンテンツ流通におけるさまざまな支援を行っています。

デジタルコンテンツを扱う同社にとって、海賊版サイトなどへの情報漏えいは大きな経営リスクになりうる要因の1つです。そこで、リスク管理の各種取り組みの1つとして、出版社とのファイルの受け渡しや社内での入稿作業といったデジタルコンテンツの出し入れが発生する業務における情報流通の動きを的確に把握するべくSplunk Cloud Platformを採用しました。

全社的なリスク管理の一環としてデジタルコンテンツ保護の取り組みを推進

コロナ禍でリモートワークを推進し、社内に展開する多くの業務基盤をクラウドリフトすることに成功している同社。現在はゼロトラストを軸にしたセキュリティ環境の整備に取り組んでおり、2023年に新設された情報セキュリティ課が中心となって、外的な脅威に対するさまざまな対策を実施しています。特にセキュリティ対策は、執行役員CIO 中野 要氏が中心となってITガバナンスの強化に向けた予算化など、事業継続に与えうるリスクの軽減につなげるための環境整備を進めてきました。「元々ID管理の基盤整備からエンドポイント対策の強化を含め、さまざまなツールを段階的に導入してきています。その過程で、各種ツールのログを集約することが検討されたわけですが、これは全社的にリスク管理を推進する中で、電子書籍を含めたデジタルコンテンツの保護が重要事項として挙がったことが背景にあります」と中野氏は語ります。

昨今では、デジタルコンテンツをインターネット上で不正に公開する海賊版サイトなどが大きな問題となっていますが、同社は取次としてデジタルコンテンツを数多く扱っているため、調達先となる出版社からデジタルコンテンツの保護を強く求められています。デジタルコンテンツの漏えいを未然に防ぐためにも、ログ集約を強化し、取り扱っているデジタルコンテンツの動きを把握するための環境整備に着手しました。

第三者機関の高い評価とクエリの柔軟性、非エンジニアでも運用できる使い勝手を評価

これまではパブリッククラウドでAWSを業務基盤のプラットフォームとして採用しており、AWS上に展開するログ分析のソリューションは活用していました。しかし、社内ネットワークやPCを含めたログの監視に関する基盤が整っておらず、それらのログと相関的に分析できる環境が求められていました。「取次基幹システムからダウンロードして検品することもあれば、取次として電子書店にコンテンツ提供するなど、デジタルコンテンツを出し入れする機会が業務上多く発生します。デジタルコンテンツの出し入れが横断的に把握でき、しっかりアラートとして可視化できる環境整備を希望したのです」と中野氏。

そこで注目したのが、収集したログの相関分析が可能になるSIEMの存在であり、第三者機関の評価が高く、統合的なログの分析基盤として豊富な実績を誇るSplunk Cloud Platformでした。OSSのログ分析ツールも検討したものの、クエリの実行に時間がかかるだけでなく、運用保守の工数が大きな負担となることが懸念点でした。「Splunk Cloud Platformであれば、SPL言語を活用することでクエリ処

成果

リスク評価
問題行動の定量的な把握でリスク評価が可能に

1時間
1日以上かかっていたログ調査が1時間以内で可能に

10倍
高速なクエリ処理で10倍以上の速さで調査に必要な情報を発見

株式会社メディアドゥ
執行役員CIO
中野 要 氏

株式会社メディアドゥ
IT統括部
シニアスペシャリスト
井上 智裕 氏

株式会社メディアドゥ
IT統括部
情報セキュリティ課
課長
三森 泰規 氏

理がとても柔軟で、曖昧な検索方法でも欲しいログが取り出しやすい。Active Directoryのログなども集約できるなど、総合的にログの有効活用が可能な点を高く評価しています」と語るのは、IT統括部 情報セキュリティ課 課長 三森 泰規氏。

また、エンジニアでなくとも導入や運用が可能な点も重視しました。「私達の部署自体が少人数のため、専門のエンジニアが関わらないと導入・運用できないものは難しい。その点、Splunk Cloud Platformであればクラウド環境で利用できますし、サーバー保守も不要です。我々にとっても使いやすい点を評価しました」とIT統括部 シニアスペシャリスト 井上 智裕氏は語ります。

結果として、デジタルコンテンツの流れを把握する環境とともに、社内に展開するネットワークやエンドポイントからのログを集約し、統合的に管理するための基盤として、Splunk Cloud Platformが選択されたのです。

> 経営層に対して情報漏えいに関する定期的なリスク報告が可能になっただけでなく、出版社からの調査依頼に対しても、根拠をもって我々側にリスクがないことを示せるようになりました”
>
> 株式会社メディアドゥ
> 執行役員CIO
> **中野 要 氏**

> 業務がしっかりと可視化できるようになっただけでなく、ログの追跡範囲が拡大し、我々が認識しづらい方法で社員が出版社とやり取りしているケースを把握できるようになり、リスクの顕在化も可能になったのは大きい”
>
> 株式会社メディアドゥ
> IT統括部
> シニアスペシャリスト
> **井上 智裕 氏**

電子書籍の入稿や取次基幹システムなどのログを収集、デジタルコンテンツの流れを可視化

現在は、デジタルコンテンツの流れを把握するべく、PCの端末操作ログをはじめ、電子書籍の入稿や書店サーバーとして利用しているSFTPサーバー、取次基幹システム、そして社内限定でファイルのやり取りが発生するSlackなどの各種ログを取り込んでおり、別途サイバー攻撃に備えてActive DirectoryやファイアウォールのログなどもSplunk Cloud Platformに取り込んでいます。

運用については、外部SoCによるMSS（Managed Security Service）を利用してログ監視を行っていますが、Splunk Cloud Platformが持つAPIを活用して調査の自動化といった環境整備を進めています」と中野氏。日々の運用は外部委託して構築したダッシュボードを確認する程度で、経営層への報告や外部からの調査依頼に対してSplunk Cloud Platformを活用して調査、レポートを作成するといった活用が中心です。外部への情報公開はこれから検討が進められる予定で、上場企業としてどんな情報を開示すべきか精査している段階です。

問題行動の定量化によるリスク評価や調査作業の大幅な工数削減を実現

Splunk Cloud Platformにてログ活用を進めたことで、具体的にいつ誰がどこでどんな情報をやり取りしているのかが把握できるようになったことが何よりの効果だと中野氏は評価します。「具体的に問題と思しき行動が定量的に把握できるため、リスク評価として測定しやすくなりました。何かあれば聞き取りも含めて個別に調査できるなど、リスクの顕在化につながったことは大きい」。

また、これまで見えていなかった業務の動きが把握できるようになったことも1つの効果に挙げています。「何が正常で何が異常なのかを見極めるために聞き取りを実施していますが、1日に何千ものコンテンツが業務のなかでやり取りされていることが改めて可視化できるようになりました。ファイアウォールのログなどから、我々が認識しづらい方法で外部とのやり取りが発生していることも顕在化し、新たなセキュリティ対策に向けた検討材料としても役立っています」と井上氏。

実際にログ調査を実施する機会がある三森氏は、以前に比べて効率的な調査が可能になった点が大きいと評価します。「例えば特定のファイルの動きを調査する場合、以前なら全端末ログの収集からサーバー内でのダウンロード履歴を確認する必要があるだけでなく、ログが膨大で一括で出すことは難しい。半年分調査するとなると1日ではとても終わりません。今はファイル名で検索するだけで1時間以内には把握できます。大きな工数削減になっていることは間違いありません」と三森氏。

使い勝手についても、サーチにて大枠でクエリを実行し、そこから特定のIPをクリックするだけでさらに絞り込みが可能になるなど、かつて三森氏自ら構築したOSSのSIEM基盤で検索していた頃に比べても10倍以上のスピードで情報に辿り着けるようになっていると言います。「エンジニアではない私でも、SPL言語を入力していると予測クエリが表示され、それに従っているだけで簡単に結果が出せる。しっかりとしたサポートの機能も充実しており、とてもありがたい」と井上氏も高く評価します。

> ファイルの流出調査には、以前はログの収集から各種サーバーでの調査などかなりの時間をかけざるを得ず、調査しきれない状況も。今ではファイル名で検索するだけであっという間に把握できます”
>
> 株式会社メディアドゥ
> IT 統括部
> 情報セキュリティ課
> 課長
> **三森 泰規 氏**

Splunk Dashboard Studioの活用とログを活用した新たな領域への展開も期待

今後については、現在外部に委託して構築したダッシュボードを、Splunk Dashboard Studioを駆使して自ら作っていきたいと語ります。「今までセキュリティアラートを担当していなかったメンバーにも引き継ぎをしていきたいと考えており、そのためには綺麗なビジュアルで見やすいダッシュボードが必要になってきます。ぜひSplunk Dashboard Studioを活用してみたい」と三森氏は意欲的です。

ログ活用という意味では、SaaS側にもダッシュボード機能が備わっているだけでなく、パブリッククラウド側でもサービスの正常性を把握するための機能が用意されているなど、Splunk Cloud Platformとのすみ分けも含めて検討が必要になってくると中野氏。「どのツールを使って何を解析したいのか、どんな証跡を調査したいのかということをしっかりと取りまとめていく必要があります。データ活用に向けたデータレイクを整備していく際にも、BIツールなどとの切り分けも含めて、しっかり戦略を立てて意志を持って切り分けていきたい」。すでに労働基準法対応に向けた労務管理に関するログ要件が他部署からも寄せられていることから、セキュリティ以外の領域にも統合ログ基盤としてSplunk Cloud Platformの活用範囲が広がってくる可能性について示唆しています。

他にも、内製化に強みを持つエンジニアを多数抱えている同社は、いずれは取引先の出版社などに対して、情報漏えいにつながる内部犯行への対策として行動証跡が把握できるような環境整備を支援するといった新たな展開も十分検討できると、中野氏は今後の展望について語りました。

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

24-job#-Splunk-MediaDo-CS-104