セガサミーホールディングス、セキュリティインシデント対応や日常的な調査業務にSplunk Enterpriseおよび Splunk Enterprise Securityを採用、幅広い用途にログを活用

課題

インシデント発生や社内外の調査依頼時などでのログ集約・分析に工数が多くかかっていた。セキュリティ対策の強化と高度化を目指しながら、セキュリティの範囲にとどまらない幅広く多種多様なログが収集できる基盤整備を目指す。

導入効果

グループ全体のネットワーク機器やサーバー機器、EDRを含めたアプリケーションログを毎日150GB程収集・分析の際にSplunkソリューションを活用。成型せずにログ投入が可能で、自動でカテゴリ別に整理できることで作業時間の迅速化を実現。

SEGA Sammy HOLDINGS

業種・業界: 製造業

ソリューション: セキュリティ、プラットフォーム

成果

150GB
グループ全体の膨大なログを円滑に収集

迅速な調査
成型前のログも、自動でカテゴリ分けができるため作業工数削減に寄与

最適なUX
カテゴリ分けされたログの整理、使い勝手の高さを評価

セキュリティ対策をはじめとした幅広い範囲のログ収集を実現するSplunk EnterpriseおよびSplunk Enterprise Security

「感動体験を創造し続ける〜社会をもっと元気に、カラフルに。〜」をミッション/パーパスに掲げ、ゲームコンテンツからトイ・映像に至るまで多種多様な遊びを提供するエンタテインメントコンテンツ事業をはじめ、遊技機事業、ゲーミング事業など、幅広いフィールドでエンタテインメントを提供しているセガサミーホールディングス株式会社。

グローバルにビジネスを展開する同社では、海外で発生したインシデントを契機に、セキュリティ対策の強化および高度化に一層注力しています。インシデント対応や日々の調査業務における効率化を目指し、幅広いログ活用を行うためSplunk EnterpriseおよびSplunk Enterprise Securityを採用しました。

セキュリティ対策の強化および高度化に向けて統合的なログ基盤の整備が必要に

WELCOME TO THE NEXT LEVEL!という中期計画のもと、更なる成長を目指す同グループは、90を超える関係会社によって構成されています。そしてグループ全体のITインフラの運用管理やガバナンス強化を推進しているのが、ITソリューション本部 プラットフォーム部 ITインフラ課です。「我々の部署では国内のグループ企業を中心にサーバーやネットワークを含めたITインフラを管理しており、各社のIT担当者と連携しながらグループ全体に向けて最適なITインフラを提供しています」と同課佐々木 芳知氏は説明します。

また、システムやネットワークの監視を通じて早期に異常を検知し、ログ分析を行いながらインシデントに対処するSOCチームの役割を担っているのが、同部 グローバルセキュリティ推進室で、新たなツールの検証や導入などグループ全体でのセキュリティ強化に向けた活動を推進しています。「セキュリティに関していえば、従来はインシデントをトリガーに動くことが中心でしたが、内部不正対策の検討も含めて、今はプロアクティブにセキュリティを考えていくことをテーマに活動しています」と語るのは同推進室 田邉 由嗣氏です。

そんな同社では、以前から各機器やシステムからログを収集し、日常的に調査業務を行っています。万一のインシデント発生時にはログを集めて状況分析を行ってきましたが、統合的にログを集約する環境が整備されていないなど運用上の課題が顕在化していました。「2010年代前半に海外で発生したインシデント調査時に、各システムからログを集めて分析するために多くの時間と手間がかかったことがありました。そこで、セキュリティ対策の強化および高度化を図るべく、環境整備が求められたのです」と田邉氏は語ります。

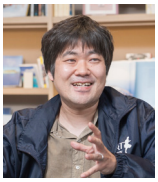
セキュリティに限定されない幅広い領域でのログを統合的に集約、活用できるSplunkに注目

新たな環境を整備するにあたっては、統合的にログを集約したうえでいち早く分析できる基盤としてのSIEMが求められました。「機器内に蓄積されているログは確かにありますが、バラバラに点在している状況にあり、それらをうまく集約するための統合的なログ基盤が必要だったのです」と田邉氏。ただし、一般的なSIEMのように、セキュリティ用途に限定された仕組み作りというよりも、同社が展開する幅広い事業領域に対応できるログ活用が可能な拡張性の高い環境整備を目指すことに。

そこで注目したのが、統合的なログ基盤として広く活用されていたSplunk Enterpriseであり、SIEMとしてセキュリティに特化した活用が可能なSplunk Enterprise Securityでした。「10年ほど前でいえば、グローバルな環境で統合的にログを集約して分析できる基盤として当時はSplunk Enterprise

セガサミーホールディングス
株式会社
ITソリューション本部
プラットフォーム部
ITインフラ課
佐々木 芳知氏

セガサミーホールディングス
株式会社
ITソリューション本部
プラットフォーム部
グローバルセキュリティ推進室
田邉 由嗣 氏



セガサミーホールディングス
株式会社
ITソリューション本部
プラットフォーム部
グローバルセキュリティ推進室
加藤 知史 氏

一択でした。また、SIEMという概念がさほど浸透していないなか、セキュリティに特化した用途として活用可能なSplunk Enterprise Securityを持っていることも評価の1つでした」と田邉氏。

特にさまざまなジャンルのゲームタイトルを開発するなどエンタテインメント領域での事業を展開する同社においては、エンジニアやアニメーターなど多様な職種のメンバーがネットワークにアクセスするだけに、一般的な企業があてはまるセキュリティ基準が適用しづらく、幅広い範囲である意味で“雑多な”ログ収集が求められます。また、外部脅威だけでなく、内部不正対策も含めて幅広く活用できるログ分析プラットフォームとしての有用性も評価したのです。

結果として、サーバーやネットワーク機器はもちろん、EDRをはじめエンドポイントソリューションも含めたログ管理の統合的なプラットフォームとして、Splunk EnterpriseおよびSplunk Enterprise Securityを導入する決断をしたのです。

社内外からの調査依頼やインシデント発生時の調査に活用

現在は、ITインフラ課が管理する同社の機器とともに、グループ会社の営業所や製造工場を含めた各拠点の1,200台を超えるネットワーク機器や800を超えるサーバー、EDRを展開する1万3,000台を超えるエンドポイントから得られる各種ログを集約しており、1日で150GBにまで達しています。また、一部クラウドストレージなどクラウドサービスのログもSplunk Enterpriseに取り込んでいる状況です。「主にインフラ系のログは取得できていますが、開発環境を含めたサービス系のログは一部のみです。予算の関係もあるため、いずれはサービス系のログもうまく統合したい。グループ企業のなかには、すでに個別にSplunkを導入して運用しているところもあります」と田邉氏。

実際の活用シーンは、内部的なものだけでなく警察を含めた外部からの調査依頼とともに、インシデント発生時のログ分析など、必要に応じて状況把握するタイミングで活用されています。グローバルに事業を展開している同社に寄せられる外部からの攻撃は少なくないため、ダッシュボード化する活用よりも都度発生する攻撃に対する影響調査などがその主な活用用途になっています。「将来的には社員のセキュリティ啓発に効果がありそうであれば、ダッシュボード化したものを提供していくことも可能性として考えられます」と田邉氏。「特にEDRからのログについては、EDR側からの検知情報だけでは詳細が分かりづらい。Splunkでうまく集約して必要な情報だけを抽出、メール通知するような活用を行っており、とても役立っています。EDR以外のログについても、Splunkで必要な情報を適切に判断できるようにしたい」と同推進室 加藤 知史氏は語ります。

> フィルターをうまく活用し、調査したい情報にたどり着きやすくなっており、検索した場合でも結果が早く表示されるため、調査時には大いに役立っています”
>
> セガサミーホールディングス株式会社
> ITソリューション本部 プラットフォーム部
> ITインフラ課
> **佐々木 芳知氏**

> Splunkに対して成型前の状態のログを投げても自動でカテゴライズされるため、ある程度の情報把握が可能です。活用までの手間をなくすことができたのは大きい”
>
> セガサミーホールディングス株式会社
> ITソリューション本部 プラットフォーム部
> グローバルセキュリティ推進室
> **田邉 由嗣 氏**

また、「内部不正などの対策については、以前に比べて意識の高まりも出てきていることから、UEBAなどと組み合わせながら活用することも将来的には検討したい」と田邉氏。

膨大なログ検索に効果的、優れたUXで使い勝手の良さを高く評価

Splunkソリューションについては、ある程度成型せずに雑多な状態でログを投げ込むことで活用できる点は大きなメリットだと評価します。「以前は個別に収集してログを蓄積しておき、必要なタイミングでログサーチできるような環境づくりに手間をかける必要がありました。Splunkを使うことで、その手間は大きく軽減できています。ログの量が膨大なため、さすがに人力だけでできる作業ではありません」と田邉氏。佐々木氏も「検索する際にもフィルターをうまく活用し、調査したい情報へたどり着きやすくなっていることは間違いありません。結果が早いだけでなく把握しやすいUIとなっており、調査時には大いに役立っています」と評価します。ユーザー体験としてのUX視点でも、Splunkが貢献している部分は少なくありません。

ログ自体の収集はもちろん、ホスト名やIPアドレス、時間などにきちんとカテゴリ分けされて整理されている点も調査時間の圧縮につながっています。「ログだけでは、ネットワークのログなのかWindowsのログなのかぱっと見ても分かりづらい。カテゴリ分けされていることで、手始めにソースを絞って確認してみるといったことがシンプルに実行できる。分かりやすさにつながっています」と加藤氏も使い勝手の面を評価します。

> EDRのログを蓄積してうまくまとめておき、必要な情報だけを抽出してメールで送るといった使い方ができるのはとても便利です。他のツールに対してもSplunkで必要な情報だけがうまく通知できるようしたい”
>
> セガサミーホールディングス株式会社
> ITソリューション本部 プラットフォーム部
> グローバルセキュリティ推進室
> **加藤 知史 氏**

また、技術面での問い合わせがあれば直接話をする機会が得られるなど、イベントも含めた積極的な情報提供なども踏まえて、Splunkとは良好な関係にあります。「直接的な問い合わせだけでなく、ユーザー数の多いSplunkだけに、インターネット上でも多くの情報が得られるのは利用者としてはありがたい」と田邉氏。

プロアクティブなセキュリティ対策に向けた環境整備に役立てたい

現状は調査用途がその中心となっていますが、現状のライセンス内でできることの幅を広げていける部分があれば、積極的に試していきたいと語ります。「ダッシュボードなどもさほどカスタマイズしていないため、他社事例も含めて我々にとって活用できる部分があれば広げていきたい」とSplunkからの提案に佐々木氏は期待を寄せています。加藤氏も「プロアクティブなセキュリティを進めていくためには、例えばすでに導入済みの脅威インテリジェンスと連携できるSplunk Enterprise Securityを活用し、サマライズされた情報をリアルタイムに届けていくといったことも可能なはず。我々が理想としている環境整備に、これからもうまくつなげていきたい」と語ります。

また顧客向けにサービス展開する事業が多い同グループは数多くの開発パートナーを抱えており、モノづくりにおけるサプライチェーン全体のリスクについても考慮する必要があります。田邉氏は今後について「サプライチェーン周りのセキュリティに対する関心も以前にも増して高くなっていることから、グループ全体のガバナンス強化とともに、Splunk活用の広がりについて期待している」と語りました。

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-SegaSammy-CS-104