他社SIEMからの乗り換えでSOC業務の効率化を実現
人的リソースの有効活用を可能にするSplunk Enterprise Security

概要

“はたらいて、笑おう。”をグループビジョンに据え、人材派遣や転職支援、ITアウトソーシングや設計開発など、総合人材サービスを展開するパーソルグループ。国内40社、海外含めて計133社のグループ会社を持ち、640を超える拠点を国内外に展開。人材派遣・アウトソーシングサービスの「テンプスタッフ」や求人情報・転職サイト「doda」による転職サービスといった人材事業に加え人材サービスとテクノロジーの融合による、次世代のイノベーション開発にも取り組んでおり、多様な働き方を推進するためのサービスを提供しています。

個人情報を多く取り扱う人材事業を展開する同グループでは、最新のテクノロジーを積極的に活用しながら、情報漏洩リスクに対処すべく情報セキュリティ対策に力を入れています。その一環として、以前から運用してきたものの柔軟性に課題のあったSIEM製品を刷新し、試行錯誤しながらグループの環境に合わせたセキュリティ脅威の検知が可能な基盤としてSplunk Enterprise Securityを採用。現在、セキュリティ分析をおこなうプライベートSOC（Security Operation Center）での業務効率化を実現しながら、迅速かつ高度なリスク分析が可能な環境を整備しています。

Splunk Enterprise Securityの採用に至った経緯をパーソルホールディングス株式会社グループIT本部情報セキュリティ部サイバーセキュリティ室 室長 持田 広志氏と同室の宮下 海里氏に伺いました。

IT環境の変化に合わせた柔軟な対応が従来SIEMでは課題に

人材事業を展開する弊グループでは、多くの個人情報を取り扱っているため、情報セキュリティ対策への積極的な取り組みに注力しており、以前から従来のセキュリティ製品単体では把握しにくい外部脅威に対して、相関分析によって検知、解析できる基盤としてSIEMを導入してきました。しかし、当時は外部脅威対策を目的にSIEMを運用してきましたが、グループ全体の事業が拡大するなかで役割の変化が求められてきました。また、SIEM以外にも様々なセキュリティ投資を行ってきており、従来SIEMの導入当時と比べて、インフラ周りのセキュリティ強化も進んできました。その結果、他のソリューションの導入が進み、外部脅威対策としてのSIEMから、今度は内部不正対策への活用を広げるなど、SIEM自体の求められる役割が変化を迎えてきたと言えます。

内部不正対策をはじめとした、自組織の環境に合わせた活用には、試行錯誤しながら運用をチューニングしていく必要があります。外部脅威対策として、ある程度決まった型がある分析ではなくなり、自組織の環境に合わせていく柔軟性が必要となったとき、従来のSIEMに課題を感じ始めました。また、外部脅威対策についても、当初はSIEMに組み込まれている検知機能だけで十分でしたが、高度化する攻撃に対応を求められる中で、取り込むべき情報や検知ロジックも多様化してきました。取り込みたいデータのフォーマットによっては、従来のSIEMでは一度取り込んだデータに対して、再度正規化や付加情報の連携をおこないたい場合、再度データを取り込み直す処理が発生するなど、運用に手間がかかっていたのも事実です。また、IT環境の変化に合わせた柔軟な対応をおこなうためには、社内でのセキュリティ人材育成が必要不可欠でしたが、ユーザー同士で情報交換できるコミュニティが十分に機能していないなど、社内で活用するための土壌にも課題を抱えていました。

そんな折、既存のSIEM製品が契約更新のタイミングを迎えたため、新たなニーズに柔軟に対応できる環境づくりに向けて、SIEM刷新のプロジェクトがスタートしました。

既存運用を踏襲しながら、スキルに依存しない使い勝手の高さが大きな魅力に

SIEM刷新のプロジェクトを始めるにあたり、課題に感じていることが他SIEMソリューションへの変更や従来SIEMの拡張やアップデートによって解決する事項なのか、それともSIEMというソリューション自体が抱える課題なのかを明らかにするため、複数の製品でPoCを実施し、実際の運用がどう変わるのかを評価していきました。これまで取得していたプロキシやファイアウォールのログ収集をはじめ、既存運用が維持可能なソリューションであることは必須条件として、製品選定のための比較を進めました。製品選定の評価ポイントは、サイバー攻撃をより早い段階で検知するような脅威検知インテリジェンスの活用や、機械学習による振る舞い検知など、新たな脅威対策が実装できることも1つでした。さらに、ユーザスキルに依存せずとも、直感的にGUI操作

PERSOL

業種

- 人材サービス

活用事例

- 外部脅威や内部不正などセキュリティインシデントの検知、調査のための基盤として活用

課題

- IT環境の変化により外部脅威対策だけの役割からSIEM自体の役割が変化
- 自組織の環境に合わせたチューニングをおこなうための柔軟性が不足
- 新規データ取り込みのハードルが高い
- カスタマイズにはシステムインテグレーターの支援が必要
- セキュリティ人材育成につなげるためのコミュニティが不足
- メンバーのスキルに依存しない直感的なGUI操作が困難

導入効果

- 多彩な分析方法によりSIEMの活用シーンも多様化
- 豊富なApps/Add onの利用による環境適応が可能
- とりあえず試してみるという、柔軟な検証が容易
- 他組織の活用事例が豊富で、内製によるカスタマイズが容易
- ユーザコミュニティなどを通した知見共有による情報収集
- Splunkでのインシデント分析を経験できるイベントによるメンバー教育
- 業務の効率化によるインシデントレスポンス対応時間の削減
- 直感的な操作から詳細な分析までメンバーのスキルに合わせた操作が可能

データソース

- ファイアウォールログ
- プロキシログ
- ActiveDirectoryセキュリティログ

ご利用製品

- Splunk Enterprise
- Splunk Enterprise Security

パーソルホールディングス
株式会社
グループIT本部情報セキュリティ部
サイバーセキュリティ室
室長
持田 広志 氏

パーソルホールディングス
株式会社
グループIT本部情報セキュリティ部
サイバーセキュリティ室
宮下 海里 氏

できるか、関連ドキュメントやUIが日本語対応しているかなど、運用をおこなう上で使い勝手の優れたソリューションであるかも検討しました。

そのなかで注目したのが、SIEMとしてグローバルで豊富な実績を持つSplunk Enterprise Securityでした。オープンソースのElastic Stackなども候補に挙がりましたが、自組織の規模でオープンソースによるSIEMの運用は現実的ではないと判断し、候補から外しています。最終的には、従来利用してきたSIEMソリューションとSplunk Enterprise Securityが選択肢として残り、コミュニティの充実度や取り込んだ後に情報が付加できるスキーマレスの運用など、試行錯誤しやすい環境づくりができる点でSplunkが高く評価されました。

また、PoCを進める中で、実際にSIEMを運用する頻度の高いSOCメンバーからも、Splunk Enterprise Securityの使い勝手の良さが高く評価されています。SPLを駆使して詳細に調査できるだけでなく、ドリルダウン形式で関連情報も見つけやすいなど、メンバーのSIEMを運用するためのスキルに左右されず、インシデント分析がしやすいという評価の声が寄せられました。加えて、SOCメンバーからは、活用のためのイベントやハンズオンセミナーなどが充実しており、新規加入メンバーでも活用がイメージしやすく、インシデント分析に対するハードルを下げることができる点も高い評価の声が挙がりました。従来のSIEMソリューションでも、ソリューション独自の構文を駆使すれば脅威ハンティングなどを実現できるとは思いますが、SplunkのSPLは汎用性が高いだけではなく、ユーザコミュニティからノウハウを得る機会が多い印象を受けています。新たに何かを実現したいと考えたとき、外部のシステムインテグレーターにサポートを依頼せざるを得ないソリューションも多いなか、Splunkはそういったノウハウが豊富ということもあり、自組織だけでカスタマイズが可能で、今後の展望を描きやすいという部分も好評でした。

最終的に、その使いやすさを十分に確認できたため、新たなSIEMとしてSplunk Enterprise Securityの選定に至りました。

ダイレクトコネクトされたAWS上に展開、環境変化に応じた新たなデータ取得も試行

現在、ダイレクトコネクトによって専用線接続されたAWS上に、クラスタ構成のIndexerをはじめ、Search Head、Forwarder、License Masterといったそれぞれのコンポーネントが構築されており、脅威ハンティングやインシデントレスポンスといった業務にデータを活用するため、SplunkのSmart Store機能を使ってS3上に格納することで、1年以上のデータ保存を実現した運用をおこなっています。日々の運用では、宮下氏を中心に10名ほどのSOCメンバーが日々Splunk Enterprise Securityに触れています。

現時点で収集しているデータに加えて、今後を見据えたSIEMの活用方法を検討し、より高い効果が見込めるデータの取得を計画しています。リモートワークが増えている昨今、それに対応したデータやEDRのプロセス関連ログやPCの操作ログなどの取得も検討しています。まだ十分に活用できているとは言えないSplunk Apps/Add onについても今後積極的に利用していきたいと考えています。Splunk Apps/Add onは、最近登場したセキュリティソリューションについても、連携できるものが多く、取り込むデータが多岐にわたっても、データを収集するための解析構文を書かずとも簡単に取り込める点が大きな魅力です。

SOC業務の効率化の実現とともに、前向きな意見が出やすい環境づくりに貢献

Splunk Enterprise Securityに切り替えたことで、以前に比べても有事の際にSIEM活用できるメンバーが増え、軽微なインシデント発生時の調査もスムーズになったと評価しています。以前は調査のたびに画面遷移が頻繁に発生するなど苦手意識を持ったメンバーもいましたが、Splunkであれば全文検索で容易に情報にたどり着けるなど、操作性が優れているという意見が多いです。調査の負担が減ることで、インシデントの因果関係調査や対応に関する見解も迅速に出せるようになりました。社内のアセット情報をSplunkに登録することで、集約的な分析を可能とする環境づくりにも取り組んでいます。業務の効率化に伴い、SOCメンバーから次はこういったことを実現したいなど、前向きな意見が出ることも増え、ポジティブな雰囲気を生み出しているという点でも効果が大きいと考えています。

SOC業務全体の効率化のために、調査に関するチケット発行などのケース管理もSplunk内で完結できるように整備も進めています。インシデントレスポンスを例にすると、ある製品でアラートを受け、そのアラートをチケット管理システムに登録し、そこから調査を始めてといった運用が多いかと思います。そういったプラットフォームが分かれていた以前の環境から少しずつ脱却することができ、インシデントのクローズ判断もしやすくなってきました。また、メンバーのスキル向上にも寄与していると感じています。例えば、既存業務の対応時間が短縮したことで、新たなセキュリティソリューションについて知見を深めることや、インシデントが発生した場合の追跡にこれまで以上に注力するための時間が確保できるようになりました。

Splunkのサポートについて、カスタマーサクセスマネージャによる支援を受けており、他社の活用事例などの豊富な情報を紹介いただくことで、弊グループのSIEM活用を考える上で有益な情報が得られています。セキュリティアナリストを対象にしたBoss of the SOCと呼ばれるCTFをはじめとしたイベントに参加することで、Splunkを利用したインシデント分析の経験を積むことや他社も含めた参加者間で情報交換できるなど、セキュリティ人材の育成にも効果を感じています。

詳細な調査をスムーズにできる環境構築とともに、自動化に向けた取り組みも検討

今後は、新たなデータを取り込むことでSIEMの活用を広げながら、詳細な調査が容易にできる環境構築にも取り組んでいきたいです。具体的には、検出したマルウェアに関する知見を得るためにVirusTotalをはじめとしたOSINT活用や社内の他システムと連携を考えています。サイバーセキュリティ室以外の部署からSplunkにデータを取り込んで活用してみたいという声も寄せられています。各部署のデータを活用することでセキュリティに限らず、自組織全体に新たな効果を生み出せないか検討していきたいです。

他社事例を見てもSplunkを活用した運用自動化のケースが増えてきており、関心が高まっています。そのため、インシデントの検知から対応、クローズに至る業務プロセスの自動実行をSplunkプラットフォーム上で可能とするSOARソリューションSplunk Phantomや機械学習を用いた行動分析により、様々な脅威や異常な行動を検出できるUEBAソリューションSplunk UBAには注目しています。

20-13742-Splunk-PERSOL-A4-102-CS-JP