パナソニック インフォメーションシステムズ、グループ全体のログレイク基盤としてSplunk Cloud Platformを採用、セキュリティやIT運用など幅広い用途への活用を加速

課題

急務となったセキュリティ対策において、統合的なログ収集のためのSIEM基盤の環境整備が必要に。セキュリティ用途に限定せず、グループ全体でさまざまな用途に活用できるログレイク基盤としての環境整備を目指し、インフラとして拡張性の高い、使い勝手の優れたソリューションを模索。

導入効果

自社が環境整備を進めるPXベストハイブリッドプラットフォームにおいて、セキュリティやベストハイブリッド運用機能を下支えする基盤としてSplunk Cloud Platformを採用。Splunk Enterprise SecurityやSplunk IT Service Intelligenceにて、セキュリティ運用やIT運用の高度化も推進。

Panasonic

業種・業界: 情報システム

ソリューション: プラットフォーム
セキュリティ、IT運用

パナソニックグループのログレイク基盤として拡張を続けるSplunk Cloud Platform

1999年に松下電工の100%子会社として設立、2015年にはパナソニック株式会社コーポレート情報システム社から事業譲受したことで、現在はパナソニックグループの国内外の多様な事業をITで強力に支援しているパナソニック インフォメーションシステムズ株式会社。Panasonic Transformation（PX）と呼ばれるDX推進を通じてグループの企業全体の価値向上に努めながら、グループのIT中核会社としてグループのB2B市場への新たな価値を提供し続けています。「カルチャーの変革」「オペレーティング・モデルの変革」「ITの変革」という3階層のフレームワークに、セキュリティも同列に位置づけPXを推進しており、なかでもITの変革においては、レガシーからの脱却やクラウドとオンプレミスの特性を活かしたベストハイブリッド、データドリブン基盤の構築、SCMの最適化などを掲げています。

そんな同社が進めるPXベストハイブリッドプラットフォームにおける、セキュリティやベストハイブリッド運用機能を下支えする基盤としてSplunk Cloud Platformを採用。Splunk Enterprise SecurityやSplunk IT Service Intelligenceなど目的に応じて必要なソリューションを活用しています。

さまざまな用途に活用できるよう、インフラチームが統合的なログレイク基盤を整備

もともとSIEM環境を整備するためのプロジェクトがスタートしたのは、2021年に発生したセキュリティインシデントがきっかけでした。マルウェア対策強化や権限の最小化、認証強化などグループをあげてサイバーセキュリティ対策の強化を推進することで、サイバー・ハイジーンの徹底を実現することになったのです。ここで検討されたのが、異常監視を行うためのSOC機能の強化であり、そのために欠かせなかったのがSIEM基盤の整備でした。「これまでもログを調査して対処する運用は行われていましたが、各所に散らばったログを人海戦術で集めて調査するような運用だったことから、迅速な調査・分析が可能な総合SOC及びSIEM基盤を整備する動きが出てきたのです」と八木氏は当時を振り返ります。

ただし、セキュリティを担当する部署は別に存在しており、インフラ運用を担当するプラットフォームサービス事業部がSIEM基盤そのものを運用するわけではありません。「実はネットワークを運用しているチームは、以前からネットワーク機器のログを収集するための仕組みを構築しており、その環境もSIEMの候補に挙がっていました」と八木氏。一方で、以前から将来的なビジョンを描く活動のなかでさまざまなログを収集・蓄積するログレイク基盤の構想が検討されてきたという事情もあったのです。「データドリブンな経営に向けた大きな方針が会社として示されているなか、ログを蓄積して活用するニーズはセキュリティに限らずIT運用のシーンにおいても今後も出てきます。目的に応じてその都度ログレイク基盤を選定していくことは非効率なため、インフラ部門としてログレイク基盤を整備するべきだと考えたのです」と八木氏は語ります。

世の中から情報が得やすく、内部的な知見も得やすいSplunkソリューションを選択

そんなログレイク基盤として注目したのが、2015年の合併以前からグループに導入されていたSplunkソリューションでした。実はオンプレミスのSplunk Enterpriseにてインシデント発生時の調査や監査対応に向けた統合ログ環境を運用していましたが、古いバージョンのままアップデートできず、ハードウェアの老朽化も進むなど課題が顕在化していたのです。「実はオンプレミスの環境を最新のクラウド環境に置き換える検討をしたことがありましたが、利用者からの強いニーズがなかったことから断念した経緯があります。クラウド化に向けて取り組みたいという我々の想いがあったなか、ちょうどSIEMのニーズが高まったことで、改めてインフラチームとしてSplunk Cloud Platformを推すことにしたのです」と飯田氏は経緯を語ります。

成果

10分
3日ほどの調査プロセスが、SPLコマンドだけで10分ほどでできる

3ヶ月
数千もの対象機器からのログ収集を含めたSIEM基盤整備をわずか3ヶ月で実現

統合
グループ全体で活用できる統合的なログレイク基盤を整備

パナソニック インフォメーションシステムズ株式会社
プラットフォームサービス事業部
プロフェッショナルサービス部
部長
八木 洋至 氏

パナソニック インフォメーションシステムズ株式会社
プラットフォームサービス事業部
インフラ標準サービス部
飯田 啓也 氏

SPL言語による検索の使い勝手が高く、相関分析しやすいなど評価の声がセキュリティチームから寄せられており、Splunk Cloud Platformへの期待が高まっていたのです。「SIEMとして広く利用されているSplunkだけに、ネット上に活用方法などの情報が数多く散見されるなど、調べやすい点は大きなポイントでした」と飯田氏。また、ホールディングス内で製品セキュリティを担当する部門でSplunkを活用していることが明らかに。「ホールディングス側でマルウェアに対する脅威検知ロジックを開発しており、SOCにもそのノウハウやロジックが活用できることもパナソニックグループとしてSplunk選択の大きなポイントの1つになったのです」と八木氏。

その結果、Splunkの基盤運用についてはインフラ部門が担当し、脅威検知ロジック開発はホールディングス、統合SoC運用は、セキュリティ部門で担当するという棲み分けでSplunk Cloud Platformの活用を進めることが決断されたのです。

> Splunkを含めたインフラを使いたい人にわかりやすく提供することで本業に集中できる環境を支援しています。事業会社のビジネスに対する貢献度は広がっていることは間違いない”
>
> パナソニック インフォメーションシステムズ株式会社
> プラットフォームサービス事業部
> プロフェッショナルサービス部
> 部長
> **八木 洋至 氏**

1日2TBのログ収集、セキュリティやIT運用など用途に応じてログレイク基盤を活用

現在は、Splunk Cloud Platformをログレイク基盤として日々2TBほどのログを収集しており、サーバやネットワーク機器などログ収集対象機器は3000台ほど、70種類ほどある各種ログをほぼリアルタイムにHeavy Forwarderを経由して収集しています。「従業員情報やネットワーク情報など変更が少ないものは1日1回ですが、多くのログは即時収集し、30分以内のログ収集を目標として運用しています」と飯田氏。

国際間に加え、イントラ網と外部接点の通信等、徐々に対象領域を拡大し、取り込み対象ログも爆発的に増えるなか、脅威検知ロジック開発を加速させるべく、Splunk Enterprise Securityを導入しています。契約当時に比べて2倍の2TBでの契約となるなど、取込み量も爆発的に増加しています。

また、基幹システムとして運用しているSAPの運用改善及び自動化や、サーバ管理部門に対してインフラが可視化できるダッシュボード提供に向けてSplunk IT Service Intelligenceを導入。「人海戦術を強いられてきたSAPの運用高度化に向けて、収集したログからSplunk IT Service Intelligenceが持つAI機能などで自動対応できるような環境づくりを進めています。当初から、PX実現の一部としてログレイク基盤の構想があり、SIEMだけでなくログレイク基盤としてグループに必要なテーマをどんどん誘致していく計画がありました。このSAPやダッシュボードに関する取り組みもその1つです」と八木氏。

統合SOCとして利用しているユーザは100名ほどですが、サーバのパフォーマンス情報などを確認するメンバーは登録者数で2000名を超える規模となっています。「我々はもちろん、実作業を行っているパートナーも含めて2000名ほどが利用していますが、これからオンプレミスで稼働するサービスを利用している事業会社への展開も計画しています。ダッシュボードについては、クラウドで稼働するサービスログも投入する予定で、多くの事業会社がクラウドにて研究開発に利用していることもあり、おそらく利用するアカウントは数万人に広がる可能性もあります」と八木氏は説明します。

わずか3ヶ月でSIEM基盤としての環境整備を実現、調査時間の大幅な短縮に貢献

実際にSplunkソリューションを導入したことで、数日かかっていた調査がわずか10分足らずで終わるなど、定量的な効果も表れています。「例えばActive Directoryのイベントログをバックアップから戻して目視で3日ほどかけて調査していたようなプロセスが、今はSPLコマンドを叩くだけで調査できます。現場からも好評です」と飯田氏。インフラ可視化のダッシュボードのおかげで、以前はサーバ利用者からリソース状況の問い合わせがあってから回答するまでに8時間ほどかかっていたものが、必要な情報にダッシュボードで辿り着けるようになり、サーバ利用者自ら状況を確認することができるようになるなど、日々の運用において大きな効果を生んでいると評価します。

今回の基盤整備については、SOCとして機能するためのログ基盤構築・一次ログ取込みを3ヶ月ほどの短期間で実施するなど、早期での立ち上げを行っています。膨大な対象機器からログを収集するために、体制づくりや役割分担などさまざまな工夫を凝らしながら、直面する技術的な課題にも適宜対処していくことで、初期の構築と展開を短期間で実現しています。「確かに立ち上げの苦労はありましたが、大きなトラブルなく基盤整備を実現できたという意味ではソリューションとして優秀ですし、クラウドとして使い勝手の高い製品だと考えています」と飯田氏は評価します。

なお、導入した当初はオンプレミスで運用してきたSplunkの知見が陳腐化していたこともあり、プロフェッショナルサービスを含めた手厚い支援を受けたとSplunk Services Japan合同会社について評価します。「営業から技術サポートを含めて精一杯努力していただいていますし、しっかり社内に持ちかえって答えを出すなど前向きな姿勢はとても評価できます」と八木氏。

> SIEM製品としてSplunkが広く利用されており、使いこなしの方法などネットからも調べやすい。内製化も視野に、我々に適したものだと判断したのです”
>
> パナソニック インフォメーションシステムズ株式会社
> プラットフォームサービス事業部
> インフラ標準サービス部
> **飯田 啓也 氏**

情報セキュリティ用途への展開を進めながら、内製化に向けた技術力強化にも取り組む

現在セキュリティ関連ではSIEM基盤としての環境整備が進んでいますが、これからもサイバー対策は継続して進めていく計画で、ホールディングスや事業会社を含めたサーバの数はさらに膨大な数が残っており、サイバー対策に向けてログ収集先は拡張していく予定となっています。「別途PCの操作ログなど内部不正などによる情報漏えい対策につながるような情報セキュリティに展開していくことも現在進めています。この試みは、国内のみならず、グローバルで標準化した取り組みとなっていくはずです」と八木氏は語ります。また以前から運用してきたオンプレミスのSplunk環境のクラウド移行も検討を進めています。「ハードウェアの限界を迎えつつあるなかで、来年度にはしっかり移行していけるようにしたい」と飯田氏。

Splunk Cloud Platformによるログレイク基盤は、1つのプラットフォームながら目的に応じて提供する先が異なってくるため、権限をうまく分離させるなど長く運用していくための設計支援に期待を寄せています。「継続的な支援は今後も期待したいところですし、我々としては社員技術者を育てていくことで、内製化に向けた技術力強化を進めていきたい。現在契約しているビジネスパートナーにもSplunk教育を順次受けてもらい、一緒になって自社リソースとして開発の内製化を進めていければと考えています」と今後について八木氏に語っていただきました。

Splunk無料トライアルまたはCloudトライアルをダウンロードしてお試しください。Splunkは、クラウドとオンプレミスのオプションを備えており、ご利用容量の規模に応じて、ご要望に合うデプロイメントモデルをお選び頂けます。

splunk>

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

Splunk, Splunk>およびTurn Data Into Doingは、米国およびその他の国におけるSplunk Inc.の商標または登録商標です。
他のすべてのブランド名、製品名、もしくは商標は、それぞれの所有者に帰属します。© 2024 Splunk Inc. 無断複写・転載を禁じます。

24-job#-Splunk-Panasonic-CS-104