初動対応も含めた説明責任を果たすための重要な基盤に 組織内CSIRTとSOCの運用に欠かせないSplunk Enterprise

概要

1949年にスポーツを通じて青少年を育成したいという創業者の思いから、神戸で生まれた鬼塚株式会社をルーツに持ち、1977年にオニツカ株式会社、株式会社ジィティオ、ジェレンク株式会社の3社が対等合併することで総合スポーツ用品メーカーとして発足した株式会社アシックス。ランニングやベースボール、バレーボール、テニスなどさまざまなスポーツの用品、用具を提供するアスレチックスポーツ事業を中心に、オニツカタイガーやアシックスタイガーなどファッション領域でのブランドを展開するスポーツライフスタイル事業、ビジネスシューズやキッズ用シューズなどを手掛ける健康快適事業など、さまざまな事業領域をグローバルに展開。「スポーツでつちかった知的技術により、質の高いライフスタイルを創造する」をビジョンに掲げ、健康で幸せな生活を実現できる製品やサービスの提供を使命として活動しています。

同社では、2015年にセキュリティオペレーション体制の整備を本格化させるべく、情報セキュリティ委員会、および情報セキュリティ事務局を発足。そして、インシデント発生後の初動対応を含めた体制づくりをさらに推し進めるべく、2016年には組織内CSIRT(Computer Security Incident Response Team)「ASICS-CSIRT」を発足させ、同時に実務としてのセキュリティオペレーションセンター（以下、SOC）の環境を整備しています。その環境づくりの一環として、点在する社内システムのログを一元管理する基盤としてSplunk Enterpriseを採用、社内に展開するファイアウォールやプロキシ、エンドポイントで稼働するEDR(Endpoint Detection Response)などの各種ログを収集、分析することでインシデントの検知能力を高め、エビデンスとなる証跡を保管することで社会的な説明責任を果たすことに役立てています。

組織内 CSIRT と SOC 環境の整備、そして EDR と連携する仕組みが必要に

2016年にインシデント対応チーム、いわゆるCSIRTを社内に立ち上げるために同社にジョインしたIT統括部 グローバル基盤チーム セキュリティリード 谷本 重和氏。入社当時は、同社内でインフラ基盤等の運用体制の整備は進められていたものの、具体的なインシデントが発生した際の初動対応などの環境整備が十分ではなかったと谷本氏は当時を振り返ります。「当時は標的型攻撃やBEC（Business Email Compromise)などのビジネスメール詐欺が広がり始めた時期です。しかし、何からのインシデントが発生しても、既存の情報セキュリティ委員会などの役割では、初動対応などを行う体制にはなっていませんでした。実質的な監視体制と初動対応を含めた、セキュリティ運用体制づくりが求められていたのです」。

そこで、これまでの職歴においてCSIRTを複数立ち上げた経験を持つ谷本氏が、組織内CSIRTとして「ASICS-CSIRT」の設置を提案、社内的にも体制づくりが急ピッチで進められることになったのです。また24時間365日の監視体制を整備するべく、マネージドセキュリティサービス・セキュリティオペレーションセンター（MSS:Managed Security Service/SOC:Security Operation Center）の導入プロジェクトも進められました。さらに、エンドポイントのセキュリティ強化に向けて、従来のウイルスソフトに変わり、EDRの導入も同時に検討することになったのです。「パターンファイルによるウイルスソフトでは防ぐことが難しい、ある意味感染するのは当たり前の時代。そこで注目したのが、ふるまいをMSS/SOCで検知し、その結果をリアルタイムに対応することが可能であるEDRでした」と谷本氏。もちろん感染した端末は潜伏期間や過去の痕跡も含めると、リアルタイムな状態だけでは判別できないものが多いと指摘します。「過去のログから証跡を確認したり、相関分析を行ったりすることで怪しい端末を特定する仕組みもEDRとともに必要でした。そこで選択したのがSplunkだったのです」と導入の経緯を語ります。

小規模でも役立つ汎用的な分析ツールになると確信

谷本氏がSplunkを知ったのは、商用SOCにおけるSIEM（Security Information and Event Management）として採用されていたことをセキュリティアナリストの経験から知っていたことがきっかけです。「規模の大小はあるものの、いわゆる小規模ながら商用SOCで行われるログの収集や相関分析が、非常に短期間かつ少ない投資で実現できるのがSplunkだと当時から理解していました。たとえ中小企業であっても役立つ汎用的な分析ツールになるはずと当時から確信しており、現実にユーザ企業にジョインしたことで、それが実現したわけです」と谷本氏。また、第三者機関が出すSIEM関連のレポートにも、Splunkがいわゆる世界的にリーダーとして位置付けられており、その実績を高く評価したのです。

asics

業種

- スポーツメーカー

活用事例

- 組織内CSIRTおよびSOCの業務基盤として活用

課題

- 具体的なインシデントが発生した際の初動対応などの環境整備が不十分
- 新たに設置された組織内CSIRTやSOCにおいて業務基盤の整備が急務
- エンドポイントセキュリティ対策としてのEDRを補完する仕組みが必要に
- 自分たちに発生している事象をタイムリーに知る環境が整備できていない
- ログの相関分析ができておらず、アラートログやイベントログを監視する術がない

導入効果

- 組織内CSIRTやSOCに必要なログ分析基盤が整備できた
- ログの自動分析によって、自社の状況がタイムリーに理解できるようになった
- 人手を介さずに、ログを自動解析してアラートが通知可能になった
- ログの証跡から、インシデントに対する説明責任が容易に果たせる環境が整備できた
- ログ分析の効率化で、社内リソースを温存しながら働く環境が改善できた

データソース

- 次世代ファイアウォール
- クラウドプロキシ
- プロキシサーバ
- エンドポイント対策としてのEDR
- クラウド上に展開するサーバのイベントログ

スプランク製品

- Splunk Enterprise

株式会社アシックス
IT統括部
グローバル基盤チーム
セキュリティリード
谷本 重和氏

特に、同社に限ったことではありませんが、ログ分析を含めたセキュリティ監視・運用業務をアウトソースしている傾向が多いことで、自社に発生している事象をタイムリーに知ることができないことも当時の課題だったと谷本氏は説明します。「実際にログを自社で利活用できていないために、ログの相関分析ができない、PC端末の異常な挙動やプロセス監視などの分析ができない、アラートログやイベントログをリアルタイムに監視する術がないといった課題が顕在化していました。当社においても、自社の置かれた状況が理解できるのは、アウトソース先からの月次レポートなどで伝えられたタイミングで、しかもセキュリティに知見のない通信会社からのレポートでは内容的に不十分。これらの課題を一挙に解決できるソリューションとしてSplunkに期待したのです」と谷本氏は指摘します。

インシデントの通知が自動化され、発生後の追跡も容易に

現在Splunkは、データセンター内のプライベートクラウド基盤に構築された仮想環境上で動かしており、社内の限定された環境でのみWebコンソールにアクセスできるようになっています。次世代ファイアウォールやプロキシサーバ、EDRなどさまざまなシステムからログを収集し、Splunk内で分析、スコアリングされた形でリスクが提示されます。SOCでの監視は24時間365日の運用体制でアウトソーシングを行っており、緊急性の高いインシデントのみ、PoC（Point of Contact)のスマートフォンへ通知される運用です。

ASICS-CSIRTでは、インシデント発生後の動きなどをログから追跡し、例えば情報漏えいのインシデントであれば、誰がいつどんな形で情報を持ち出したのかの流れをSplunkによって、ログ解析や調査をする運用となっています。「SOCの運用を社内の人材だけで行うと過重労働となりかねないため、働き方改革の観点からも外部に監視業務を一部アウトソーシングする体制を整備しています。Splunkによって人手を介さずにログを自動解析してアラートが通知されるようになっており、運用にかかる時間や工数を減らしながら、正確に処理できるようになっています」と谷本氏は説明します。

初動対応としての説明責任が果たせる“コスパの良さ”を高く評価

日々のセキュリティ業務に利用しているSplunkですが、「何かインシデントが発生した場合でも、ログの証跡からきちんとした説明責任が果たせる最低限の環境が整備できた」と谷本氏は評価します。「個人情報はもちろん、例えば靴のデザインやその製造プロセスといった知的財産の漏えいにつながるようなものは、当社の外部からの攻撃だけに限りません。社内の内部犯行も含め、その情報がどう移転していったのか、ステークスフォルダに対して上場会社として、説明責任が伴います。Splunkによってログを分析し、その証跡が負担なく示せるのは大きな効果。しかも、デジタルフォレンジックの専門的な経験や技術がなくても、上司や経営層にすぐに伝えることができます。非常にコストパフォーマンスの高い製品」と谷本氏。なお、Splunkによってログ分析が効率化できるようになったことで、経営効率化の名のもとに人を切ることなく、社内リソースをそのまま温存しながら働く環境が改善できるようになった点も見逃せないと谷本氏。

Splunk はランナーと一緒に手を携えるトレーナーのような存在

Splunkの魅力について谷本氏は「他製品との親和性も高く、当社のようなユーザ企業のビジネス環境に対しても、柔軟にフィットしてくれる点です。またベンダー市場の中でセキュリティ活用以外にも、強いイニシアチブを持っており、巨大なITベンダーのように買収を繰り返すこともない。ホリゾンタルではなくバーティカルに、ユーザ企業へのビジネスパートナーとして、Win-Winな関係で付き合えることも私には合っています」と力説します。また器であるSplunkだからこそ、周辺ツールとコラボレーションすることで大きな効果を発揮してくれる点も魅力の1つだといいます。「リアルタイムな検知を可能にするMSS/SOCとEDRとの連携もSplunkならでは。ランナーが一緒にトレーナーと手を携えてゴールを目指す、つまりは強力なツールをSplunkが支えながら、企業に大きな効果を与えてくれる存在です」と谷本氏は評価します。今ではセキュリティ業務の中心にSplunkがあり、それぞれ相関的に結び付けている状況です。他にも、Splunkを通じて導入企業とコミュニケーションする機会が増えているという副次的な効果も。「我々が本社を構える神戸では、まだユーザーコミュニティが東京ほど成熟しておりませんが、我々の活動がその一助になればと考えています」と谷本氏。

内部不正対策の強化に向けた積極的な脅威のハンティングを加速

今後については、内部不正対策という視点で新たなソリューションについても検討したいと谷本氏は語ります。「プライバシーの問題はありますが、行動監視やふるまいなどを逐一把握することで、情報漏えいや不正な持ち出しについての迅速な対策も必要です。そこで、積極的に脅威のハンティングを行いつつ、事前サービスの面でASICS-CSIRTを強化するべく、サービスの充実を図りたいと考えています。そこで将来的には、Splunk User Behavior Analytics (UBA) のような仕組みについても興味を持っています」と谷本氏は語ります。また、現状の活動は、国内を中心とした展開ですが、海外も含めた形でガバナンスを強化するための仕組みも検討していく必要性を感じています。「一部海外領域でのログもPoC (Proof of Concept) としてSplunk内に展開していますが、2018年5月に欧州で成立したGDPR (General Data Protection Regulation) や中国におけるサイバーセキュリティ法など、ログの移転が難しい部分も出てきています。リージョナルなSIEMを各国に設置するといった、新たな時代に適した工夫も必要になってくるはず」と谷本氏。

ログを含めたビッグデータ解析という世界では、同社がメインとしているスポーツ関連のビジネスに役立てるようなアプローチにも期待を寄せていると谷本氏。「実は、野球の硬式ボールにセンサーを内蔵した投球測定用ボールを提供しています。このセンサーから得られるビッグデータを記録更新のためのアプローチに役立てることもできるはず。業界を活性化させる手段の1つとしてSplunkが活用できることを社内にも広めていきたい」と今後について谷本氏に語っていただきました。

20-13890-SPLK-ASICS-A4-103-CS-JP