無償で使えるSysmonにてエンドポイントの可視化を実現 セキュリティ兼任組織でも脅威への初動対応の迅速化を可能にする Splunk Enterprise

概要

“二木の菓子”として有名な株式会社二木が手掛けるゴルフ用品販売事業からスタートし、現在は関東を中心に、北は北海道、南は福岡まで、全国50を超える店舗を構えている株式会社二木ゴルフ。ゴルフ専門店のみならず、オンライン販売や中古クラブ専門店、提携するゴルフ場のインショップなどゴルフに関連した事業を幅広く展開、顧客向けのレッスンやフィッティングなど各種サービスも提供しています。「ゴルフを楽しむお客様をサポートする」という方針をもとにゴルフを楽しむ文化の醸成に尽力しており、経営方針である「顧客第一主義」を念頭に、さまざまな施策に取り組んでいます。

そんな同社においてシステム部門の役割を担っているのが、坂井 滋 氏が所属する情報システム課です。「セキュリティ兼任組織で運用している関係上、可能な限り省力化が可能な仕組みを整備しながら、安心かつ安全に利用できるシステム環境の構築を行っています」と説明します。特にセキュリティ面では、顧客から預かった個人情報などを安全に管理すべく、店舗で利用するPOS端末への対策をはじめ、アンチウイルスソフトウェアや操作ログの取得が可能な資産管理ツールといったエンドポイント保護対策、ファイアウォールなどの境界防御、ネットワーク型Sandbox製品による脅威検知など、さまざまなセキュリティ対策を実施しています。これらセキュリティ製品のログを自動的に収集し、インシデントの検知や原因究明の際に活用するSIEMとして導入されたのがSplunk Enterpriseです。

各ソリューションのログをそれぞれ確認するなど、原因特定に時間がかかる

顧客第一主義を掲げる同社において、個人情報を含めた情報保護対策は重要な施策の1つ。高額所得者も少なくない顧客層をターゲットにしているゴルフ業界だけに、強固なセキュリティ環境を整備していくことが求められています。そこで外部脅威に対処すべくさまざまなセキュリティ対策を実装してきた同社ですが、少人数で運用していることもあり、インシデント対応を効率的に実施できる環境整備が急務だったと坂井氏は当時を振り返ります。「Sandbox製品でアラートが検知されると、さまざまな製品のコンソールにアクセスしてログを確認し、その原因特定を進めることになります。このインシデント発生後の初動対応の段階で多くの手間と時間が発生していたのです」。官公庁をターゲットにした偽メールが日本国内で蔓延した際には、エンドポイントの調査に多くの時間がかかり、原因究明が困難な場面も。原因特定が難しいグレーなケースでは、早急にPCを抜線したうえで回収して再セットアップを施す必要があり、インシデントが終息するまでに数か月を要したこともあったほどでした。

小さく始めることができ、使いやすさから少人数でも十分運用できる点を評価

そんな環境を打開するべく以前から注目していたのが、統合的にログを収集し、分析可能なSIEMでした。「エンドポイント対策としてEDR製品をテスト的に導入してみましたが、セキュリティに関する高度な知識やノウハウが必要で、これ以上エンドポイント対策に投資することも難しい状況でした。そこで、コストをおさえながら効率的に運用できる仕組みとして目をつけていたのがSIEMだったのです」と坂井氏。なかでも注目していたのがSplunk Enterpriseでした。また「EDRの代わりにMicrosoftの無償ツールであるSysmon（System Monitor）を活用することで、エンドポイントのログも含めて統合的に管理できるという提案をいただきました。ログ量での課金だけに、小さく始められる点も我々が求める規模感に最適な構成になると考えたのです」と坂井氏は評価します。

使い勝手の面でもSplunk Enterpriseを高く評価した坂井氏。「端末名を入力するだけで、ある程度の情報が一覧で表示され、必要に応じて資産管理ツールやSysmonのログなど絞り込んで調査していくことが可能です。SQLの知識さえあれば、サーチコマンドからパイプでつなげていくだけのシンプルな仕組みで利用できる。製品に精通した知識を習得せずとも運用できるのはとても魅力的でした。さほど詳しくない人間でもそれなりに使えますし、少人数で運用する意味でも我々として十分使いこなせると判断したのです」。

そこで、社内の環境にて半年間ほどのPoCを実施したことで実運用に生かせることを確認、

NIKI GOLF

業種

- スポーツ関連小売業界

活用事例

- セキュリティ対策製品の統合的なログ管理、解析

課題

- インシデントの初動対応に時間と手間がかかる
- セキュリティ兼任組織でも負担なく運用できる仕組みづくりが急務
- エンドポイント対策への新たな投資が難しい
- 知識習得の十分な時間が確保できない

導入効果

- サーバーリソースのリアルタイムな状況把握が可能
- インシデント対応の工数を1/4ほどまで削減
- 初動対応の迅速化で被害を最小限に防止することが可能に
- 業務を止めることなく安心安全な環境づくりに貢献
- 状況が容易に可視化でき、心理的な負担軽減にも寄与
- 豊富なSplunk AppsとAdd onによって活用の幅が容易に拡大できる
- ログが活用できるかどうか試行錯誤しやすい

データソース

- Sandbox製品
- ファイアウォール
- Sysmon（System Monitor）
- Active Directory
- アンチウイルスソフトウェア
- 資産管理ツール
- AWS CloudTrail
- Amazon CloudWatch
- 基幹システムのサーバログ

ご利用製品

- Splunk Enterprise

株式会社二木ゴルフ
経営企画室
情報システム課
坂井 滋 氏

各種セキュリティログの統合的な管理による万一のインシデントにおける初動対応に役立つソリューションとして、Splunk Enterpriseが採用されたのです。

セキュリティログやサーバーのリソースログなどから状況の可視化を容易に実現

現在は、PCやサーバーを含めた300台を超えるエンドポイントに無償のSysmonを展開しており、アンチウイルスソフトウェアや資産管理ツール、Sandbox製品やファイアウォールなどの各種センサー、Active Directoryをはじめとした認証ログなど、セキュリティ関連のログを中心に、会計システムなど基幹システムのリソース管理のためにログ情報をSplunk Enterpriseにて収集。業務で利用しているニフクラ（旧ニフティクラウド）やAWSといったパブリッククラウドサービスの操作及び監査系のログ取得も行っています。ログ自体は5Gほどが日々蓄積されており、1年後に破棄されていく運用です。

具体的な活用としては、Sandbox製品でアラートが発生した時点で、各センサーから寄せられたSplunk Enterprise内のログを相関的に分析していく流れです。また、現在はリソース管理の一環として、基幹システムが稼働するサーバー群のCPU・メモリ利用率などの情報をSplunk Enterpriseにて一元的に収集しており、サーバーのコンソールにアクセスせずともほぼリアルタイムにリソースの可視化が可能になっています。「基幹システムに何かあれば、保守契約先にリモートで確認してもらう運用体制となっており、その際にはコンソールが占有されてしまって我々が状況把握できないケースも。今はSplunk Enterpriseでログを取得しているため、コンソールを奪い合うことなく迅速に状況把握できます」と坂井氏は評価します。

インシデント対応の工数を大幅削減、心理的な負担軽減にも貢献

Splunk Enterpriseを導入したことで、インシデント対応の工数が大幅に削減されたと坂井氏は力説します。「担当者2名が2時間かけて調査していたものが、今では私のほうでSplunk Enterpriseからログを確認し、30分ほどで初動の調査が可能となりました」。短時間で解析できるようになったことで被害を最小限におさえることが可能となり、従業員の業務を止めることなく安全安心な環境づくりに一役買っています。「各ソリューションそれぞれに手を出さずに済むようになり、スキル習得のための手間も減らすことができました。状況の可視化も容易で、心理的な負担が大きく軽減しています」と坂井氏は高く評価します。

Splunk Enterpriseについては、多くのSplunk AppsとAdd onが用意されており、自社の環境にも容易に適用できる点が大きな魅力の1つだと語ります。「現在運用しているポータルの切り替えを検討しているのですが、新たな環境でログ取得するためのAppsがすでに存在しています。もしポータルの情報が取得できるようになれば、新しい活用も広がるのではと期待を膨らませています」と坂井氏。新たなログ情報が必要になっても、ログ転送のためのエージェントであるユニバーサルフォワーダーがエンドポイントに展開されており、後から必要な情報を手軽に収集できる点も評価するポイントの1つに挙げています。さらに、スキーマ定義を事前に行うことなくデータが投入できるため、使えるかどうか試行錯誤しやすいと好評です。

収集ログを増やしてセキュリティ強化へ、ビジネスに貢献できる基盤としても期待

今後については、IP情報からユーザを特定できるようDHCPサーバーのログをはじめ、手作業にてWebサイトからダウンロードしないと投入できないメールサーバーのログも自動的に取り込めるような仕組みづくりなど、セキュリティ対策へのさらなる強化を図っていきたい考えです。「効率的にインシデント対応できるよう、セキュリティ運用におけるタスクの自動化が可能なSplunk Phantomなどもぜひ検討したい」と坂井氏。必要があれば、WAFやIDS／IPSといったセキュリティ関連のログを拡充していきたいと語ります。

また、現状はセキュリティ関連のログやサーバーのCPU負荷といったIT運用に関するログが中心ですが、売上に貢献できるような仕組みづくりにもSplunk Enterpriseを活用していきたいと意欲的に語っています。セキュリティを中心とした守りのITだけでなく、売上貢献できる攻めのITに脱却していくためのツールとしても期待を寄せています。「基幹システム内に蓄積されている顧客情報や売上ログを取り込むことで、システム部門としてビジネスに直接貢献できるような情報を社内に提供していきたい。現状は実店舗とオンライン上の顧客基盤が別になっていますが、これを統合的に見ていくことで、新たな気付きにつながるような情報の可視化に役立てていきたいですね」と今後について語っていただきました。

20-13742-Splunk-IT-Nikigolf-A4-102-CS-JP