splunk> listen to your data™

CASE STUDY

三井物産セキュアディレクション株式会社

統合ログ監視システムの構築で脅威をいち早く検出、解析して対処

Splunkを導入したMBSDのユーザ企業では、最大4週間かかっていたマルウェア感染などのインシデント対応を数時間に短縮

「10社の機器を使っていれば、10種類のログが出てきます。従来のログ監視システムでは初期設定に多くの時間を費やしていました。Splunkは機器によるログフォーマットの差異を自動で吸収し、そのまま取り込むことができます。直ちに分析可能な状態となりますので短期開発を実現できます」

三井物産セキュアディレクション株式会社
マネージドサービス事業部 部長代理
斎藤 博樹 氏

OVERVIEW

業種
- ITサービス業

課題／背景
- ログを収集し、鳥瞰的に事象・脅威を捕らえる仕組みの実現
- 事象や予兆をいち早く検出・解析
- 原因・影響範囲を効率よく特定し迅速に対処
- SOX法やIT監査に対応した、発見的統制の実現

ソリューション
- Splunkを採用した統合ログ監視システムの構築

導入効果
- 他社製品に比べ開発期間を約2分の1に短縮
- 洗練されたダッシュボードで分析およびレポート作成を効率化
- 最大4週間かかっていたマルウェア感染などのインシデント対応を数時間に短縮

データソース
- メール
- プロキシ
- アンチウイルス
- IDS/IPS
- ファイルサーバ監査
- ファイアウォール
- など10数種類のログ

※1 Private Security Operation Center
※2 Computer Security Incident Response Team

最高水準のセキュリティプロ集団を目指すMBSD

「ITリスクマネジメントのリーディングカンパニーとしてお客様を安心へ導き、ネットワーク社会の未来作りに貢献いたします。」という企業理念に基づき、2001年3月に設立された三井物産セキュアディレクション株式会社（以下、MBSD）。情報セキュリティの診断・監視や、ITリスク・情報漏えい対策などの各種セキュリティ・コンサルティング、また、顧客自身がセキュリティの運用管理を行うP-SOC※1およびCSIRT※2の構築支援も行い、総合的なセキュリティサービスを展開しています。

『分析』に主眼を置くプロ用ツールとして採用

これまでのセキュリティ対策は、アンチウイルスやファイアウォールに加え、システム環境に応じてIDS/IPS、WAFなどの様々なセキュリティデバイスを多段に設置し、強化が図られてきました。しかし外部からの攻撃は日々多様化し、また悪意の有無に関わらず、内部からの情報漏えいやマルウェアなどの感染の被害が増大しているというのが現状です。マネージドサービス事業部 部長代理の斎藤博樹氏は、次のように語ります。

「アンチウイルスやファイアウォールなどの基本対策に加えて、セキュリティデバイスを多段に設置するという原理原則は間違っていないのですが、それだけではセキュリティの脅威は防げなくなってきています。外部からの攻撃者は、メールやWebサイトを悪用し、巧妙にセキュリティデバイスをすり抜け、内部にマルウェアを送り込みますし、そもそも内部に不正行為を行う者がいるかもしれません。こうした状況下、セキュリティデバイスによる強化策だけで大丈夫だという常識が崩れているのが実情です」

そこで、セキュリティデバイスはもちろんのこと、システム全体で利用されているIT機器やアプリケーションなどのログを収集し、点を線でつなぐことにより、侵入の目的や影響の範囲などをいち早く解析して、脅威に迅速に対応しなければなりません。斎藤氏は、「ログを収集し、鳥瞰的に事象を捕らえるためには、できるだけ多くのログを効率的に収集し、高速に検索できるツールが必要でした」と話します。

MBSDでは2012年6月より、統合ログ監視製品の比較検討をした結果、Splunkの採用を決定します。採用の理由をコンサルティング事業部 ITセキュリティグループ マネージャーである後藤久氏は、「攻撃やその予兆は、膨大なログの中にほんの一握りだけ足跡を残します。セキュリティ専門家は顧客のIT環境や刻々と変換する状況を見極め、複雑な条件を組み合わせ、分析を進めます。Splunkは、専門家の高度な要求に対し、膨大なログから、いとも簡単に脅威を可視化また特定できます。操作は直感的で、まさに『分析』に主眼を置くプロ用のツールであると感じました」と話しています。

導入障壁低く、P-SOCやCSIRTにも適用

Splunkを活用するメリットを斎藤氏は、次のように語ります。「10社の機器を使っていれば、10種類のログが出てきます。従来のログ監視システムでは、ログフォーマットの変換処理が必要で、専任の開発担当者が初期設定に多くの時間を費やしていました。しかしSplunkはログフォーマットの差異を自動で吸収し、そのまま取り込むことがで

マネージドサービス事業部　部長代理
斎藤 博樹 氏

コンサルティング事業部
ITセキュリティグループ　マネージャー
後藤 久 氏

MBSDのセキュリティ・オペレーション・センター（MBSD-SOC）では、お客様のサイトを24時間×365日体制で監視し、侵入などの脅威が発生した場合には、迅速に対処・対策します。

無料ダウンロード

Splunkは無料でダウンロードができます。1日500MBまでのデータのインデックスを作成でき、Splunk Enterprise のあらゆる機能を60日間無料でお試しいただけます。無料期間終了後でも期間中でもいつでも、無期限のトライアルライセンスへの切り替えやEnterpriseライセンスの購入が可能です。今すぐライセンスの購入をご希望の場合は、以下のメールアドレスよりお問い合わせください。
お問い合わせ先：**splunkjp@splunk.com**

きます。直ちに分析可能な状態となりますので短期開発を実現できます。話を聞いたときには信じられませんでしたが、実際に使ってみて驚きました」

また後藤氏は、「他社の製品ではダッシュボードにまで気を配っていないことが多いのですが、Splunkのダッシュボードは非常に洗練されています。ブラウザ上で、専用コンソールと同等の高い操作性が実現されています。またレポート機能も充実し、カスタマイズの幅も広く、目的に沿ったレポート作成も容易に実現できます」と話します。

今後の取り組みについて斎藤氏は、「お客様自身がセキュリティの運用管理を行うP-SOCやCSIRTにおいてもSplunkを活用し、体制構築を支援していく計画です。そのためのサポートを、引き続きSplunkには期待しています」と話しています。

ユーザ企業の標的型サイバー攻撃対策にSplunkを採用

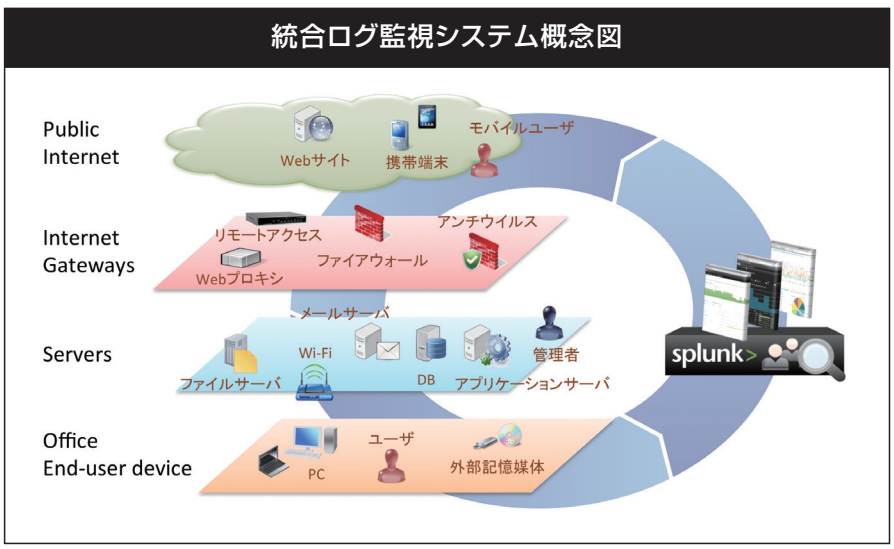
MBSDでは、標的型サイバー攻撃へ適切に対処するには、統合ログ監視システムによる脅威の可視化と迅速な対応が重要であるとし、そのコアツールとしてSplunkを採用。MBSDが構築した統合ログ監視システムについて斎藤氏は、次のように語ります。

「いままでは、各サーバやセキュリティデバイスは、それぞれ異なるベンダーにアウトソースされ、もちろんログも別々に管理されていました。標的型サイバー攻撃の観点から、お客様環境のリスクアセスメントを実施し、ログ収集対象をファイアウォールなどのインターネット境界に設置される全てのセキュリティデバイスに加え、アンチウイルスや重要情報が格納されるサーバ群としました。それらのログをリアルタイムに収集・蓄積し統合的に管理・分析するための仕組みを構築しています」

この仕組みでは、1日あたり約50GB、1万5000名分のログを収集。斎藤氏は、「朝刊約100年分の情報量を1日で蓄積する分量です。この大量のログから、不正なアクセスや挙動を抽出し、事実関係や影響範囲を特定します。また、リスクアセスメント結果やお客様環境の特性などを踏まえ、なりすまし行為などの発生条件を洗い出し、Splunkの柔軟な検知ロジックのルール化機能を用いて自動化を実現しています」と話します。

後藤氏は、「Splunkを導入する前はウイルスが見つかるとログを収集し、原因を突き止め、完全に収束するまでに最大で4週間かかっていました。Splunkを導入したことで、ウイルスを発見して数時間でシステムを修復できます。また今後は、Splunkの適応範囲をSOX法やIT監査にも拡大し、発見的統制を実現していく計画です」と話しています。

統合ログ監視システム概念図



Splunk Services Japan合同会社　〒104-0031 東京都中央区京橋1-3-2 モリイチビル3階　splunkjp@splunk.com　www.splunk.com