SIRTの処理のフローをWorkbookで定義、可視化を実現 SIRT運用の高度化を支援するSplunk SOAR

概要

三井物産セキュアディレクション株式会社（MBSD）は、セキュリティに関する防御の計画から事前対策、検知、事後対応まであらゆるシーンに対応可能なセキュリティソリューションをサービスとして備えており、官公庁やグローバル企業などエンタープライズ領域の顧客に対するセキュアな環境づくりを支援しています。従業員の多くがセキュリティに関するコンサルタントおよびエンジニアで構成されており、なかでも高度なサイバー攻撃をログなどから発見する脅威ハンターやマルウェア解析技術者といったセキュリティエンジニアが数多く在籍する、セキュリティのプロフェッショナル集団です。

そんな同社では、顧客のシステム全体を顧客内部のSOCとして監視するAdvanced SOCでログからのThreat Huntingなどによる脅威検知からセキュリティ機器の遮断まで自動化を実現させています。一方で、顧客SIRT（Security Incident Response Team）の一員として運用支援などを手掛けていますが、インシデントなどの機微な情報も扱うSIRT運用においても人手による処理に関するフローを定義し、その状況を可視化できるサービスマネジメントの環境整備が求められました。そこで、Workbookにおけるケース管理によって対応フローが定義でき、SIRTで発生したイベント情報など各種情報を可視化する環境づくりに向けてSplunk SOARを採用。脅威インテリジェンスとの連携によって、セキュリティ対応の自動化による脅威対策も合わせて実現しています。

プライベートSOCの構築などニーズの変遷に対応するべく Splunk Enterpriseを導入

市場におけるセキュリティへの要求は、経営環境とともに大きく変遷を遂げています。以前はセキュリティ製品の運用をアウトソースしたいというニーズが強かったものの、ここ数年では社内のシステムおよびネットワーク全般をどうセキュアに保つのかというプライベートSOCの構築・運用などに大きくニーズが変遷している状況にあります。そんな状況下で、高度なセキュリティエンジニアが数多く在籍する同社では、これまでSOCサービスを運用するために欠かせない、SIEMも含めた基盤全体を自社開発してきましたが、ニーズの変遷に対応するべく新たな基盤を模索したとコンサルティングサービス事業本部長 兼 公共事業部長 関原 優氏は説明します。「自社開発のSIEMだけに、お客様の要求に応じて新たなセキュリティデバイスのアラートやログ格納・監視対応などのサポートに必要な機能を開発してきましたが、外部の新たなソリューションへの対応も含め、保守し続けるには大変な工数が発生していました。そこで、自社で柔軟に運用できる基盤への刷新を検討するなかで、データの収集・検索する基盤として強力なツールだったSplunk Enterpriseに注目したのです」と関原氏は当時を振り返ります。

複数のSIEMやログマネジメント製品を比較した結果、Splunk Enterpriseであれば、スキーマ定義が不要なことと高速なデータ収集および検索が可能な仕組みとして最適だったのです。「新たなセキュリティデバイスのサポートを行うために、とりあえずデータを入れてスキーマを定義せずにスピーディに分析できれば、顧客の要望にも応えやすい。まさに、高速処理が可能なSplunkが適していました」と関原氏。現在も顧客の要望や環境に応じてさまざまなSIEMを運用していますが、同社が主体的に基盤整備を行う際には、Splunkエキスパートが数多く在籍しており、過去蓄積してきた分析ルールの活用が柔軟に可能であることからもSplunk Enterpriseが選択されている状況です。

SIRT運用におけるフローの定義、 可視化に最適だったSplunk SOAR

そんな同社が手掛けるプロジェクトのなかで、グローバル展開する企業において課題と

MBSD

業種

- IT業界

活用事例

- SOC運用における情報収集、分析基盤、SIRTにおける状況の可視化およびオペレーションの自動化

課題

- 顧客ニーズの変遷に応じて自社開発環境からの脱却を目指す
- SIRT運用でのフロー可視化、自動化などサービスマネジメントの強化
- SOCで自社開発されたSOARのみではSIRTでの活用が難しい

導入効果

- SIRT運用におけるフローの定義、自動化を実現
- SOC運用だけでは得られない、価値の高い情報提供が可能に
- 脅威インテリジェンスとの連携によるメールフィルターの自動運用を実現

データソース

- ネットワーク・セキュリティ機器からのログ
- 送受信情報をはじめとしたメール関連ログ
- アプリケーション稼働ログなどサーバ関連ログ
- ID登録から削除までを含めた各種認証ログ
- 端末操作など端末関連ログ
- 脅威インテリジェンス

ご利用製品

- Splunk Enterprise
- Splunk SOAR

三井物産セキュアディレクション株式会社（MBSD）
コンサルティングサービス
事業本部長 兼 公共事業部長
関原 優 氏

なっていたのが、社内に設置されるSIRT運用におけるサービスマネジメントでした。「実はSOCの領域では、オペレーションの自動化に寄与するSOARを自社開発していましたが、機械的な検知をベースに分析するSOCよりも、インシデントなどの機微な情報を扱うSIRTについてはシステムを用いて全体管理できる環境が整備できていませんでした。特にSIRTでは、電話やメールなど人間系の対応にどれくらいの時間がかかっているのか、外部に対してどこまで情報を開示するのかといった人手による処理を可視化する環境が求められます。SIRTとSOCを連携させながらも、個別管理が必要なSIRT領域を我々が運用するSOCの仕組みで吸収するのが難しかったのです」と関原氏は語ります。

そこで検討したのが、イベント管理をはじめ、Workbookによるケース管理やレポートによる可視化が可能なSplunk SOARでした。「お客様で利用されているサービスマネジメントソリューションを活用することなども検討しましたが、リージョンごとに異なるソリューションを利用しているお客様だったため、統合するのがそもそも難しい状況でした。そうであれば、SIRT側でSplunk SOARを活用し、その仕組みと柔軟に連携させていくほうが最良だと考えたのです」と関原氏。

その結果、同社が提供する顧客セキュリティ組織運用支援におけるSIRT運用においてイベント管理や可視化およびケース管理の基盤として、Splunk SOARが採用されることになったのです。

SIRT運用のフローをWorkbookにて定義、処理の自動化もあわせて実現

現状は、同社が提供するセキュリティサービスにおいて、SOC運用に欠かせない、ネットワーク・セキュリティ機器から得られるログをはじめ、メールやDBログ、アプリケーション稼働ログ、認証ログ、端末操作ログ、組織情報、アセット情報、脆弱性情報、特権利用申請ログなどあらゆる情報がSplunk Enterpriseをベースに構築・開発された独自のSIEMプラットフォームにて収集、分析されています。また、従来マニュアルで運用されていた情報収集から把握、調査、SOCへの指示、対処までのSIRTでの運用フローをSplunk SOARのWorkbookにて定義し、自動化を図っています。さらに、同社が運用する脅威インテリジェンスからもたらされる情報をSIRTにて受領し、事前に定義されたルールに沿って自動的な対処も行われています。

具体的には、不審メールが着弾する前にメールフィルターにて遮断ルールなどに自動反映させるといった活用です。「以前はSOC側では着弾したメールの行動をウォッチするなど、後追いでの防御が中心でしたが、今は脅威インテリジェンス側で不正ドメインが取得されたことを迅速に検知し、Splunk SOAR側で自動対処しています。自動的な防御が可能となったことで業務そのものが大きく効率化できています。一方で、サービスマネジメントにおける可視化については、Splunk SOAR上で対応履歴などを残したうえで、設定されたKPIの達成度合いを可視化していく試みも進めており、今後Splunk Enterpriseとの連携も進めながら実現していきたい」と語ります。

経営層などに対して価値の高い情報提供を推進

Splunk SOARを活用することで、SIRTの運用履歴を経営層に対してより容易に提示するなど、価値の高い情報が顧客に提供できるようになっていくとことを期待しています。「SIRT側ではSOCでは対応しない未遂レベルの情報も含めたものが集まるため、企業のリスクとしてインシデント全体の状況を定量的に示して認識いただくことで、さらなる投資につなげていただくなど、ビジネス的な側面でメリットが得られると考えています」と関原氏。

Splunk社には、エキスパート人材によるサポートが手厚く行われており、同社と一緒になって能動的な支援が得られたことを評価しています。「Splunk SOARについても導入前から各所で調整を密に行っていただき、しっかりフォローいただいており、満足しています」と関原氏。

さらなるSIRT運用の高度化を推進、DX支援など新たな領域にも展開

「SOCの領域については自社での作り込みも進んでおり、顧客の要望に応じて柔軟な拡張を続けていますが、SIRT運用についてサービスマネジメントやインシデントマネジメント、そして企業ガバナンスの領域までカバーしていただけるような、さらなる柔軟性がSplunk SOARに備わってくることを期待しています」と関原氏。

また、マルウェアの行動分析など高度なスキルを持つデータアナリティストが多数在籍している同社だけに、企業のDX支援に人材を転用するという新たな方向性についても見据えています。「特にSplunkを扱うセキュリティアナリストは、さまざまなデータの特性をとらえて、データ突合や分析ルールを作成できるため、お客様社内のデータを扱うことで、DXに転用するための分析が可能な状況にあると考えており、既に大手顧客の一部では、セキュリティのために収集したデータから、企業価値を上げるためのデータ活用の検討を進めています。既にセキュリティ対策で収集しているデータをセキュリティエンジニアが活用し、DX支援に貢献できるという認知度を向上させていきながら、今後はSplunkによるセキュリティ以外のユースケースを積極的に提示していきたい」と今後のビジネス展開について力強く語っていただきました。

21-13742-Splunk-IT-MBSD-A4-102-CS-JP