Customer Case Study

SWIMLANE

柔軟性の高いSOARの導入により、セキュリティの監視運用の自動化、一元化、効率化を実現

TOSHIBA

東芝グループは「人と、地球の、明日のために。」という経営理念のもと、長年にわたって社会インフラ事業を手がけてきました。経営理念には「人」、「地球」、「明日」という三つの要素が入っていますが、これは人類のみが恩恵を受ける世界ではなく、「人類」と「地球」が永続的にバランスを取りながら、より良い世界を創っていきたいという想いの表れです。そして昨今では、創業以来培ってきた製造業としてのフィジカルの技術と、情報およびAIを中心としたサイバー技術を融合したサイバーフィジカルシステムテクノロジーによって、社会インフラを支えることをミッションとして事業を展開しています。

課題

東芝には現在、サイバーセキュリティセンターという部門があり、昨今の情報セキュリティのリスクの高まりに伴い、2017 年に設立されました。同組織は情報セキュリティに加え、自社の製品、システム、サービスに対する製品セキュリティも対象とした東芝グループ全体のセキュリティを支えるミッションを担っています。サイバーセキュリティセンターでは、リスクベースでセキュリティ対策を進めており、「全社のリスクをきちんと把握し、脅威インテリジェンスを活用しながら、セキュリティの監視運用をどう効率的に行っていくかが私たちの課題になっていました」と、株式会社東芝　技術企画部　サイバーセキュリティセンター　セキュリティ戦略室 参事の小島 健司（こじま けんじ）氏は振り返ります。

さらに昨今では脅威が複雑化・巧妙化し、インシデントも増加していく一方で、IT 環境やセキュリティ対策の手法も複雑になってきており、いかに効果的に運用していくかが当面の重要な課題となっていました。また、セキュリティに関する十分な知識・スキルをもつ人材も不足しており、限られた人数で知見を集約・可視化し、効率よく運用していく必要もありました。サイバーセキュリティセンターにおいては、「発生したセキュリティインシデント情報について集約管理していましたが、より効率的な運用のためにはそれらの情報を活用した管理を強化していく必要があると考えていました。また、システム間の連携強化も 1 つの鍵と考えていました」と、株式会社東芝　研究開発センター　サイバーセキュリティ技術センター　セキュリティ運用推進部　参事の大橋 俊道（おおはし としみち）氏は語っています。「セキュリティでは過去の失敗から学び、きちんと改善につなげることが重要であり、そのためには管理の仕組みから変えていく必要があると考えていました」（小島氏）。

ソリューション

サイバーセキュリティセンターではこうした課題を解決するため、対策を検討し始めましたが、ちょうど SOAR（Security Orchestration, Automation and Response：セキュリティのオーケストレーション、オートメーション、レスポンス）製品が出始めた時期だったため、５社ほどの SOAR 製品をリストアップし、比較検討を開始しました。その中で 3 社の製品に絞って機能を詳細評価し、PoC（概念実証）も行いつつ、同センターの求める要件を満たすかどうかを確認しながら製品選定を進めていきました。SOAR 製品の選定で評価したポイントとしては、外部製品やサービスとの連携性や運用のしやすさ、およびベンダーとしてのサポート体制、あるいは同センターの要件に対して、カスタマイズを容易に行えるかどうかといったカスタマイズ性を重視しました。特にこれからプロアクティブなセキュリティ対策を行っていく中で、脅威インテリジェンスとの連携が非常に重要だと考え、脅威インテリジェンスをきちんと SOAR の中に取り込んでセキュリティの中で活用していくことが容易にできるかどうかが重視されました。

導入

最終的にサイバーセキュリティセンターが選んだ SOAR 製品はスイムレーン（Swimlane）でした。「SOAR で重要なポイントは、我々の思い通りにプレイブックを構築できること、そして運用結果をきちんとダッシュボードで共有できることが重要だと思っています。スイムレーンはプレイブックやダッシュボードのカスタマイズ性が非常に高いという点が一番大きな選定理由です」と小島氏は説明しています。スイムレーンでは、ダッシュボードを自由に組み替え、見たい KPI を容易に表示できるといった特長があります。「他社製品だとプレイブックがあらかじめデフォルトで決まっているものがプリインストールされている感じだったんですけれども、スイムレーンは柔軟に自分で多彩なプレイブックのタスクの流れをカスタマイズできました」（大橋氏）。スイムレーンの導入時には、事前に机上の検討だけでなく PoC も行っており、工夫したポイントとしては、あらかじめ SOAR の上に載せたいユースケースを定義し、きちんと手順を可視化しておくことで、スイムレーンでの実装を比較的スムーズに行うことができました。

効果

スイムレーン上にインシデント情報を集約することにより、現在の状況を速やかに把握することができるようになり、ダッシュボードで管理することで、社内で共通認識を得ることが容易になりました。また、現状の KPI を迅速に把握できるようになったため、それに基づいた運用の改善を実現しています。実際の運用においては、スイムレーンと脅威インテリジェンスツールを連携させ、インシデント対応で不審な IoC が見つかれば脅威インテリジェンスで調査し、運用にフィードバックすることでインシデント対応をスムーズに行うことができるようになりました。このように一つ一つの作業を効率化することで、全体としての作業時間の削減に成功し、節約できたリソースを他の作業に充てることが可能になりました。

「例えば、いろいろなところからセキュリティ上危険な URL や IP アドレス情報を随時各所から入手していますが、入手した情報に対して東芝の従業員がそれらの URL にアクセスした形跡のログを調査する作業が発生します。こうした作業はスイムレーン導入前では、それぞれのネットワーク機器のログを手動で見に行って、検索用のコマンド入力していました。スイムレーン導入後では、IP アドレスを入力するだけで該当するアクセスログがないかを調べて、その結果をスイムレーン上で確認できるようになり、作業のスピードと手間が大幅に改善しました」（大橋氏）。

株式会社東芝
技術企画部
サイバーセキュリティセンター
セキュリティ戦略室
参事 小島 健司氏

株式会社東芝
研究開発センター
サイバーセキュリティ技術センター
セキュリティ運用推進部
参事 大橋 俊道氏

今後

サイバーセキュリティセンターの運用の中でも、自動化できるユースケースが各種あるため、現在はインシデント情報を集約し、少しずつスイムレーンの方に取り込んでいる状況であり、今後もユースケースの自動化を拡大していく予定です。また、小島氏は次のようにコメントしています。「セキュリティ製品は非常に多岐にわたっており、各種製品と容易に連携できることが重要なポイントだと思いますので、今後もセキュリティ製品やグループウェアなど幅広い製品との連携プラグインが継続的に提供されることを希望しています。また、私たちのセンターでは情報セキュリティだけでなく、製品セキュリティも対象としています。製品セキュリティで重要となるのは、世の中で新しく発見された脆弱性に対して、自社製品のどの部分が影響するのかいち早く把握することです。今後スイムレーンを製品セキュリティにも活用していければと思います。」

SWIMLANE

Swimlane Japan

〒 102-0074
東京都千代田区九段南 1-6-5
Appedia 内
TEL：090-2734-5574
EMAIL：info@swimlane.jp

【Swimlane（スイムレーン）について】

スイムレーンはクラウド型のローコードに対応したセキュリティ自動化分野におけるリーダーです。従来の SOAR 以外のユースケースにも対応し、慢性的に人材不足のセキュリティチームの煩雑な業務プロセスや膨大なデータ処理をサポートします。また、セキュリティ部門全体の記録システム（System of Record）として機能するローコード対応プラットフォームを提供することで、各担当者のセキュリティの知識と専門性を存分に生かすことが可能となり、SOC 運用にとどまらない自動化の可能性を提供します。
詳細は www.swimlane.com、LinkedIn、Twitter をご覧下さい。