S&J株式会社 様

分散していたセキュリティ運用の仕組みを可視化・一元化 属人性が解消され、開発者以外も開発が可能に

SWIMLANE

導入事例

User Profile

S&J

社名　:S&J株式会社
所在地　:東京都港区新橋1-1-1 日比谷ビルディング8F
導入時期　:2025年5月
URL　:https://www.sandj.co.jp/

2008年11月設立のサイバーセキュリティカンパニー。「お客様の期待を常に考え『ありがとう』と言われるセキュリティサービスを提供する。」という企業理念のもと、サイバーセキュリティのエキスパート集団として、国内企業に最適化されたMXDRサービスに加え、インシデント対応の実行支援や影響分析、CSIRT組成支援など、幅広いセキュリティサービスを提供。事業成長のインフラとして機能することを目指している。

S&J株式会社
取締役
コアテクノロジー部長
半澤 幸一 氏

S&J株式会社
コアテクノロジー部
情報セキュリティスペシャリスト
久我 孝明 氏

S&J株式会社
コアテクノロジー部 コアテクノロジー研究グループ
Tech Lead　- Product & Infrastructure
大坪 竜斗 氏

S&Jが抱えていた課題

- セキュリティ運用の仕組みが案件によって異なり、管理・保守に工数がかかっていた
- ベンダーフリーという基本方針により多様な製品を扱っているため、連携が複雑化
- 属人化やサイロ化により、どのアナリストがどんな対応をしたのか可視化に手間がかかっていた

Swimlaneによる解決

- 分散していたセキュリティ運用の仕組みをSwimlaneに一本化、担当者の負荷も軽減
- ローコードでPlaybookの開発が可能となり、開発スピードと品質も向上
- 対応履歴を一元化でき、個々の作業量も容易に把握可能に

「多種多様な製品との連携実績があること、
ローコードでPlaybook開発ができることなどを評価しました」

S&J株式会社 コアテクノロジー部 コアテクノロジー研究グループ
Tech Lead　- Product & Infrastructure 大坪 竜斗 氏

従来の課題

SOCサービスの運用において工数の増加や管理・保守の複雑化／属人化が課題に 開発者以外でも扱える自動化基盤の導入を検討

S&Jは、株式会社ラック元代表であった三輪信雄氏が2008年に設立したサイバーセキュリティカンパニー。ベンダーフリーを基本方針とし、製品の提供にとどまらず、コンサルティングからセキュリティ監視、事故対応までを一貫して提供。また、自社開発によりEDRにマネージドサービスを一体化させた国産MDRサービス「KeepEye」を提供するなど、高い技術力を大きな特徴としている。同社の目指すところについて、取締役 コアテクノロジー部長の半澤幸一氏は「『技術』と『コミュニケーション』を融合させたセキュリティサービスをより多くのお客様に提供できるよう、日々努力を続けています」と語る。

さて、同社では、顧客に提供するSOCサービス（セキュリティオペレーションセンター）の運用において、工数の増加や、管理・保守の複雑化／属人化といった課題を抱えていた。コアテクノロジー部 コアテクノロジー研究グループのエンジニアである大坪竜斗氏は「運用負荷を軽減するためのSOAR（Security Orchestration, Automation and Response）のような仕組みはあったのですが、それぞれの担当者が案件ごとにPythonやC++などで独自開発したものであったため、かえって管理・保守に多くの工数がかかっていました。以前は人手に依存した運用でも対応可能でしたが、案件の増大や組織の拡大に伴ってオペレーションも煩雑になってきており、いずれは限界を迎えるだろう、という危機感がありました」と振り返る。

近年、同社は年率20%を超える高い成長を続けており、顧客数も増加の一途を辿っている。また、ベンダーフリーを基本方針とし、顧客の要望に合わせて多様なセキュリティ製品を扱っているため、それらの連携もより複雑になっていた。

「案件ごとに開発したSOAR では ドキュメントの質が統一されておらず属人化していることがあり、こうした場合、担当者を変更したり

退職してしまうと引き継ぎも一苦労です。当社は技術力の高さを強みとしていますのでリバースエンジニアリングでの対応も可能ですが、そのたびに解析を行っていては大きな負担になってしまいます。そこで、こうした課題を解決すべく、開発者ではないアナリストでも扱える自動化基盤と、可視化に優れたプラットフォームの導入を検討することにしました」（大坪氏）

なぜSwimlaneだったのか

多種多様な製品との連携実績、ローコードでPlaybook開発が可能 開発体制や課金体系も評価し採用を決定

2024年5月、S&Jは自動化基盤の検討をスタート。数多くの製品をリストアップし、これらについて慎重に比較・検討を進めた。

「当社ではベンダーフリーを掲げており、実際に複数のセキュリティ製品を併用しています。そのため、他製品との柔軟な連携機能を備えていることを要件としました。加えて、運用保守の属人化を排除するため、Playbook（インシデントの分析および対応の手順書）ができる限りローコードで開発しやすいことも重視しました」（大坪氏）

製品Aの場合、ケース管理に外部ツールを必要とするため、SOC運用との整合性が取りづらいことから見送りになった。また製品Bは、利用形態がSaaS限定のため、オンプレミス運用を必要とした同社の要件に合致しなかった。そして製品Cは、機能面は優れていたものの、ユーザー単位の課金体系だったため、同社のように50程度のアカウントを必要とする体制ではコストが非常に高くなってしまうという問題があった。

かくして数々の製品が脱落していく中、最終的に選ばれたのがセキュリティ運用の自動化ソリューション「Swimlane Turbine（スイムレーン ターバイン、以下 Swimlane）」である。

「SwimlaneはITSM（IT Service Management）製品の連携機能について調査していた際にリストアップされ、有力候補となりました。採用の理由ですが、多種多様な製品との連携実績があり、連携コネクタの柔軟性が高いこと。ローコードでPlaybook開発ができるため、開発者だけでなくアナリストも活用できることなど、当社が求める要件をすべてクリアしている点を評価しました。また、新たなコネクタが必要な際も数週間程度で開発が可能という迅速な開発体制、イベント単位の課金体系であることもポイントでした」（大坪氏）

導入の効果

セキュリティ運用が可視化・一元化され、負荷も軽減 属人化が解消され、開発スピードと品質が向上

Swimlaneの導入効果としては、第一にセキュリティ運用が可視化され、誰が何を行ったのか明確になったことが挙げられる。

「従来は管理対象が非常に多く、対応履歴を一元的に把握することが難しい状況でした。アナリストごとに使用している管理台帳も数多く存在し、業務の全体像や貢献度を把握するには複数のデータを個別に確認する必要がありました。Swimlaneの導入により、対応履歴が一元化され、業務プロセスの可視化が進んだことで、アナリスト一人ひとりの対応状況や成果を明確に把握できるようになりました。これにより、チーム全体のパフォーマンス評価にも活用できるようになりました」（大坪氏）

アラート管理も一元化された。かつては各ツールの画面を同時に確認する必要があり、時には顧客のコンソールまで見に行っていたことから、開くWebブラウザが数十に及ぶこともあったという。

「これもSwimlaneにより一元化され、非常にスッキリしたかたちで管理できるようになりました。アラート情報をポーリングしてログなどを分析する際も、個々に検索する手間がなくなりました。ケースによってはクロージングまでを自動化してくれるので、かなりの負荷軽減になっています。さらに、CSIRTとの連携も円滑になりました」（大坪氏）

アナリストの精神的な負荷が軽減されたことも大きなメリットだ。

「確認する画面が数十にも及ぶと、もしかしたらチェックを見落とすかもしれないという大きなプレッシャーがありました。これが1つの画面に集約されたことで、以前ほど神経を使うことなく管理できるようになりました」（半澤氏）

属人化という課題についても、ローコードでのPlaybook開発が可能になったことで、開発者ではないアナリストも自動化に取り組めるようになった。結果、開発のスピードが大幅にアップし、Playbook自体の品質も向上したという。コアテクノロジー部で情報セキュリティスペシャリストを務める久我孝明氏は「ローコード活用のもうひとつの効果が、開発の流れが明確になったことです。おかげで仕様書やドキュメントの作成といった作業を最小化でき、その分のリソースをより生産的な業務に振り向けられるようになりました」と説明する。

将来の展望

生成AIの利活用を慎重に検討 人とAIの強みを融合した セキュリティ運用を目指す

S&Jは今後について、生成AIの利活用を視野に入れているという。ただし、同社のようなManaged Security Service Provider（MSSP）の立場からすると、検出精度や顧客への説明責任という点で課題があり、現時点ではAIに任せた運用はリスクが高いため、慎重な姿勢で取り組む方針だ。この点について大坪氏は「人手による管理・支援を第一にしつつ、適切な範囲でアシスタント的に活用していくつもりです。社内ではすでにドキュメント検索や開発サポート用途での導入が進んでいますので、今後はお客様ごとのエスカレーション内容や分析履歴など、蓄積されたデータを活用した最適な対応案（Recommendation）の生成に役立てていきたいですね。そのためにも、Swimlaneの『Hero AI』機能を活用し、人とAIの強みを融合したセキュリティ運用を目指していきたいと考えています」と語ってくれた。

株式会社マクニカ　Swimlane担当

お問い合わせ　045-476-2010　swimlane@macnica.co.jp
https://www.macnica.co.jp/business/security/manufacturers/swimlane/

〒222-8563 横浜市港北区新横浜1-5-5
TEL.045-476-2010　FAX.045-476-2060

西日本オフィス　〒530-0005 大阪市北区中之島2-3-33 大阪三井物産ビル 14階
TEL.06-6227-6916　FAX.06-6227-6917

MACNICA

@Macnica, Inc.　●本カタログに掲載の製品仕様は、予告なく変更する場合があります。予めご了承ください。　●本カタログに掲載されております社名および製品名は、各社の商標及び登録商標です。