SUCCESS STORY

TrendAI™ Service One Completeで、アラートへの迅速な対応+負荷軽減と有事の対応フロー整備を実現

株式会社ツムラ https://www.tsumura.co.jp/
東京都、日本 | 連結:4,229名（2025年3月31日現在）
ソリューション:TrendAI™ Service One Complete

※Trend Service One Completeは、TrendAI™ Service One Completeにサービス名が変更になりました。

導入の背景

1893年に初代 津村重舎 氏が婦人薬·中将湯で創業後、現在では医療用漢方製剤を主力とする製薬企業となった株式会社ツムラ(以下、ツムラ)。医療用漢方製剤市場では、国内シェア8割以上を占め、国内の支店·営業所を中心に国内外で73拠点を展開している。

そのツムラの情報システムを所管するデジタルソリューション部では約30名体制で、情報システムの企画、開発、保守、運用、そしてリスク対応やセキュリティといった範囲をカバーしている。

「生命関連企業として、患者様、医師の先生方に漢方製剤を確実にお届けすることが企業の使命です」と語るのは黄 氏だ。ツムラでは「一人ひとりの、活きるに、生きる。」を究極的に成し遂げる事業の志(パーパス)として掲げた、理念経営を実践している。このパーパスを実現するために生産·製造を支える根幹として情報システム基盤は安全·安心·安定した運用が求められている。「情報システムが止まったから漢方製剤が提供できない、ということがあってはなりません。安定供給を確実に、継続的に、実現するために、日々の運用を確実に実施するだけではなく、インシデントの対応についても常に考えを巡らせ、アップデートをして備える必要があると考えています」と黄 氏が語る。

導入効果:

- S1C導入により、セキュリティ専門家が24時間監視し、重大なアラートのみを抽出·通知。迅速な対応と業務負担軽減を実現。
- 自社環境に存在する悪用される可能性のあるリスクを正しく把握したうえで、実運用も考慮し優先順位をつけて対処。

「安定供給を確実に、継続的に、実現するために、日々の運用を確実に実施するだけではなく、インシデントの対応についても常に考えを巡らせ、アップデートをして備える必要があると考えています」
黄 承圭 氏
株式会社ツムラ 経営統括本部
デジタルソリューション部 運用推進課 課長

従来の運用体制では、異なるベンダーの製品をレイヤー別に導入するベスト·オブ·ブリードという考え方を踏まえた上で、1つのベンダーに運用監視を委託していた。

しかし、連日サイバー攻撃による被害の報道がなされる中で、改めて自社の体制を顧みた際に以下の2点を課題として感じていたという。

1つ目は、ITシステムの運用監視を担うベンダーからの情報連携のタイムラグ。運用監視をしていたメインベンダーはセキュリティ専任の組織ではなく、インフラ環境を含むIT全般の業務も担っていたため、セキュリティ対応をあまり優先できず、情報共有にタイムラグが生じてしまっていた点。

2つ目は、有事対応フローの未整備。サイバー攻撃の脅威が高まる中、インシデント発生時の対応フローや判断基準、社内の連携体制の強化·見直しがされていなかった上、相談先となるような外部のセキュリティ専門組織との事前調整も不十分だった点。

これらの課題を踏まえ、ツムラはセキュリティ対策の一元化を検討。また、「やるべき」である必須事項と「やったほうがよい」の推奨事項の線引きが難しい現状を考慮し長期的な視点で一貫した対応を相談できるパートナーの選定を進める方針を定めた。

TrendAI™ Service One Complete(以下、S1C)の導入を決定した理由としては以下が挙げられる。

- EPPの技術を長年提供し、高いシェア率を持つトレンドマイクロがEDRを提供していることから、技術的な信頼性が高い点。
- 使用するセキュリティ製品とそれを用いた監視サービスを同じベンダーで統一することで一貫性を確保できる点。
- 打ち合わせや提案を重ねる中でトレンドマイクロが自社に有効な提案を行ってくれるパートナーとして信頼できた点。
- S1CがMDRに加えて、インシデントレスポンスのサポートや、平時のアドバイザリーのサービスも提供する点。

丹羽 剛祐 氏
株式会社ツムラ 経営統括本部
デジタルソリューション部 運用推進課 課長補佐

金井 英統 氏
株式会社ツムラ 経営統括本部
デジタルソリューション部 運用推進課 課長補佐

今後の展望

ツムラは、情報システムの安定運用をさらに強化するため、有事対応の仕組みの高度化とシステム全体の最適化に向けた取り組みをトレンドマイクロとともに継続して取り組んでいく。

最終的には人に依存しないレベルにまでフローを作り上げていきたいと考えている。そうすることで、適切な対応が素早く取れる体制の構築、迅速な意思決定、それらによる被害の最小化の実現を目指す。

また、マニュアル作成の過程で浮上した「既存システムの最新状態を常に把握し続けることの難しさ」についても、今後の課題として取り組んでいく。例えば、IPアドレスの管理など、システム資産に関する情報の継続的なアップデートには膨大な工数がかかることを改めて認識した。今後は、このような管理業務の負担を軽減するための製品の導入も視野に入れ、さらなる効率化に取り組む。

これらの取り組みを通じて、ツムラは「安全·安心·安定」した情報システムの構築をさらに推進し、漢方製剤の安定供給を支えるIT基盤の強化に努めていく。

サイバーセキュリティの取り組みを一歩先へ

株式会社ツムラのような組織が、TrendAI Vision One™ を活用して、どのように「リアクティブ」から「プロアクティブ」なセキュリティへと進化を加速しているのかをご紹介します。

TrendAI™ について

TrendAI™ は、トレンドマイクロのエンタープライズ向け事業部門であり、AIセキュリティのグローバルリーダーです。AIの包括的な可視化と統合セキュリティの提供を通じて、組織に確かな信頼をもたらし、イノベーションを推進するとともに、リスクを最小化します。

現在、世界185か国において大手企業や政府機関に採用され、アイデンティティ、インフラ、データに至るまで、組織全体を横断したセキュリティを提供しています。AI Fearlessly.

https://trendaisecurity.com/ja

導入効果

S1Cとはトレンドマイクロが提供している「お客さまのセキュリティ運用を包括的に支援する」サービスである。24時間365日体制の監視サービス、インシデント発生時のサポート、そしてセキュリティ運用改善に向けた総合的な支援を行っている。

1つ目の課題のアラート通知のタイムラグについて、S1Cの導入によってセキュリティの専門家による迅速な監視と通知を実現できた。迅速なだけではなく、トレンドマイクロでアラートを確認し、重大なもののみを抽出して通知することで、安全性を担保しつつ業務効率の向上に寄与している。実際にインタビューのタイミングでは過去1カ月で26件のアラートが上がっていた。これらのアラートをすべて自社で都度対応する必要がないという点も高評価につがった。

2つ目の課題である有事対応フローの未整備についてもS1Cを活用し、トレンドマイクロの支援を受けながら有事対応マニュアルの作成を進めている。以前、有事対応のフローやマニュアルについては、一般的な情報を収集しながら独自に整備を試みたこともあるという。しかし、公開されている情報は玉石混交であり、自社環境に最適な内容を取捨選択し網羅的に準備することの難しさを実感していた。そこで、トレンドマイクロが提供する標準テンプレートを活用しながら、自社の運用に適した形へとカスタマイズを進めている。

この過程で特に重要な気づきとなったのは、単にマニュアルを整備するだけでは十分でなく、実際の運用時にスムーズに機能する体制を構築することが不可欠であることだ。例えば、セキュリティに関連する部署だけでなく、営業部門、人事総務部門、そして経営層などにもインシデント発生の際の対応フローについてあらかじめ情報共有を行うことで、有事の際の情報共有を円滑にして社内の混乱を防ぐこと、また全社的に連携してより効率的にインシデント対応を行える効果が期待できる。

このような取り組みを経て、ツムラは有事対応の実効性を高めるための基盤を着実に構築中だ。トレンドマイクロとの協力を通じて、技術的な防御体制の向上だけでなく、組織としての対応力を強化することの重要性を改めて認識し、今後も継続的なアップデートと改善を図っていく方針である。

詳細はこちらから
https://trendaisecurity.com/ja