SUCCESS STORY

業務効率の向上を目的としたIT戦略拡大に際して、今後増加が想定されるIT資産とその安全性の徹底的かつ継続的な可視化を実施。

株式会社全日警 https://www.zennikkei.co.jp/

東京都、日本 | 警備業 | 4,874人

ソリューション: TrendAI Vision One™ Cyber Risk Exposure Management (CREM)、ウイルスバスタービジネスセキュリティサービス

※Trend Vision One - Cyber Risk Exposure Managementは、TrendAI Vision One™ Cyber Risk Exposure Management (CREM)に製品名が変更になりました。

導入の背景

日本全国で常駐警備をはじめ、競技場や各種催物の警備、貴重品運送、建物の保守、警備機器・警備システムの販売まで、幅広いセキュリティ事業を展開しているのが株式会社全日警である。

社会的に重要なインフラのセキュリティも担う事業の形態上、物理的なセキュリティに加えてサイバーセキュリティの確保も重要な命題と位置付ける同社では、SaaSやクラウドインフラを含むITの利活用にも慎重な姿勢を取り、厳格なセキュリティポリシーで安全性を第一に社内ITを運用している。限られたIT管理リソースで最大限の安全性を確保するために、社内クライアントやサーバの運用を外部委託で徹底するとともに、クライアントに導入したEDR（Endpoint Detection and Response）もMDR（Managed Detection and Response）サービスが利用可能な製品を選択し、24時間365日の監視を徹底してきた。

導入効果:

- IT資産とそれぞれのセキュリティリスクの可視化により、社内全体のセキュリティ状況が継続的に確認可能。
- 可視化された各端末のリスク数値は、端末管理を委託する外部ベンダとの脆弱性対策をめぐるコミュニケーションでも活用。
- 今後ITの利活用やDXを推進するにあたって、セキュリティ面での土台整備。

「セキュリティにおいて、そこにあるかもしれない危険に目をつぶるようなことは、決してあってはならないと考えています」

商品開発部 開発二課 課長代理 兼 経営企画室 情報システム部 情報システム課 課長代理

お客さまの課題

全日警では、業務効率向上に向けたIT利活用を本格化させていく検討が進む中で、管理すべきIT資産が今後さらに増えていくことを見据え、改めてセキュリティの在り方を見直す必要性を感じるようになっていた。「セキュリティ投資については、これまでもしっかりと行ってきました。経営層の意識も高く、安全性の確保を最優先にITを運用してきたと思います。ただ、ITをどう活用していくかという点では、まさにこれからという状況でした」と、同社情報システム部長は語る。

IT利活用の拡大を検討する中で、同社が強く意識していたのが、セキュリティリスクを見過ごしてしまうことへの不安だった。社内の既存クライアントやサーバについては、外部委託によって常に最新の状態を維持する運用を行っていた。しかし、日々新たに発見される脆弱性に対して、「それが自社のどのIT資産に影響するのかを、すぐに把握できているのか」という点には、課題を感じていたという。

さらに、IT利活用の拡大に伴い、「管理や監視の対象から漏れてしまうものが出てくるのではないか」という懸念もあった。こうした現場の問題意識が、IT資産全体を継続的に可視化し、リスクを把握できる仕組みの必要性を同社に強く意識させることになった。

選定理由

ASM(アタックサーフェス管理)という考え方については、以前から認識していたという。「Web上で提供されている診断サービスを利用して、公開ドメインや公開サーバの安全性を確認することは、以前から行っていました」と、情報システム部長は語る。診断サービスを通じて、全日警単体だけでなく系列企業や同業他社の公開ドメインを確認する中で、自社のセキュリティレベルが高いことは把握できた一方、その評価が一時点のものであり、継続的な安全性を補償するものではないという課題も見えてきた。「継続的に状況を把握できる仕組みが必要だと感じていました」

こうした課題意識を背景に、同社のセキュリティパートナーから紹介されたのが、自社環境が外部の攻撃者からどのように見えているかを可視化するツール、Cyber Risk Exposure Management (CREM)である。CREMは、公開ドメインの状態など、外部から見た自社の状況を把握、可視化し、脆弱性などを指摘してくれる点に加えて、社内クライアント、サーバの脆弱性の可視化、管理ができる点から、CREM導入の検討が始まった。さらにこれまでクライアントを中心としたEDRとしてウイルスバスター ビジネスセキュリティを利用していたこともあり、「信頼性の高い日本企業でもあることから、あえて他のASMベンダを検討することは考えていませんでした」と、同社情報システム部 情報システム課 課長代理は説明し、またMDRで同社セキュリティを監視、信頼できるパートナーから合わせてCREMのサポートも得られることから、トレンドマイクロのセキュリティプラットフォームであるTrendAI Vision One™ で提供されるCREMの採用が決定した。

ソリューション

全日警では、警備隊が利用するクライアントパソコンを含め、日常業務で使用するクライアントおよびサーバにEDRを展開、マルウェアやランサムウェアの対策を行なっている。加えてこれらの端末はCREMによるASMの監視対象としており、日々脆弱性の有無を監視、必要な対応を行なっている。また外部ドメインの安全性の監視、確認もCREMを活用して継続。さらにトレンドマイクロのAIセキュリティプラットフォームTrendAI Vision One™ のダッシュボードで全日警の社内、社外の安全性を総合的に表示するスコアを参照し、日々のセキュリティ状態の継続的な把握もおこなっている。

今後の展望

重要インフラ、社会的に重要なイベントの物理的なセキュリティを担う同社にとって、お客さまを守ることは最大の命題である。お客さまとその情報を守りつつ、さらなる業務効率の向上、安全性を高めるために、同社では積極的なITの利活用、環境の刷新を検討する方向である。現在の脆弱性の監視を中心とした運用に加えて、同社の環境に合った運用、機能の利用に全日警では期待を寄せるとともに、CREMの活用による業務効率化とセキュリティのバランスに積極的に取り組んでいく方向だ。

導入効果

CREMの運用を開始したところ、TrendAI Vision One™ の表示するリスクを表す数字も継続して低く、改めて同社のセキュリティ状況が良好であることが最初に確認できた。社内のクライアント、サーバについても基本的には最新のセキュリティパッチが当たっており、緊急で対応が必要な危険な端末が多数見られる状況ではなかった。パッチが未適用のサーバもいくつかあったが、すでに把握済み、再起動待ちのサーバであると確認できた。「社内のクライアントとサーバが一覧表示されますが、その中でも重要度、深刻度の高い脆弱性を持つ端末が最初に表示されます。早急に対応が必要な端末が明確になるので、外部委託している管理者にも効率的に現状の確認を依頼、迅速な対応ができています」と情報システム部 情報システム課長はその効果を評価している。

「社内のクライアントとサーバが一覧表示されますが、その中でも重要度、深刻度の高い脆弱性を持つ端末が一番最初に表示されます。早急に対応が必要な端末が明確になるので、外部委託している管理者にも効率的に現状の確認を依頼、迅速な対応ができています」

経営企画室 情報システム部 情報システム課長

サイバーセキュリティの取り組みを一歩先へ

株式会社全日警のような組織が、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。

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

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