SUCCESS STORY

SaaSやクラウドの積極利用でビジネスを推進するタニタが、EDRによる脅威の早期検知、対応を、積極的なサイバーリスクの管理で強化

株式会社タニタ　https://www.tanita.co.jp/
東京都、日本 | 家庭用・業務用計量器などの製造・販売 | 約1,200人（グループ）
ソリューション: TrendAI Vision One™ Cyber Risk Exposure Management、Email Security R2 あんしんプラス（トレンドマイクロパートナー提供のクラウド型メールセキュリティサービスとして）、ウイルスバスタービジネスセキュリティ あんしんプラス（トレンドマイクロパートナー提供のEPP、EDR、Managed EDRサービスとして）
※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

体組成計、クッキングスケール、温湿度計など、健康計測機器の製造・販売を行う株式会社タニタ（以下タニタ）は、これまでも顧客管理、業務システムなど自社に合ったSaaSを積極的に導入するとともに、クラウドプロバイダも活用。業務におけるIT活用を非常に活発に進めている。これまで社内で管理していたオンプレミスのサーバも、クラウド上に移行し、「持たずに活用する」の考えのもと、利便性と運用効率を高めている。この点は生成AIの活用についても例外ではなく、契約しているビジネス向けクラウドサービス群で提供する生成AIのブラウザ上での利用を推奨している。社風として前向きなIT利用において、セキュリティについても仕組み、人の両方から継続的に対策を行っている。新型コロナウイルス感染症拡大によるリモートワークへの移行によってSaaS利用、クラウド利用が進んだことを受けEDR（Endpoint Detection and Response）製品としてエンドポイント対策製品を導入するとともに、MDR（Managed Detection and Response）サービスによる、万が一の侵入時の対策を行っている。さらにセキュリティベンダによる社内勉強会、フィッシングメールの訓練を定期的に行うなど、人の面でも対策には力を入れている。

「公開資産だけでなく、社内の資産も含め、継続的に脆弱性などの状況が把握できる点は、当社の求めていた対策像に合致していました」
宮澤 裕之 氏
情報システム部 課長代理

導入効果:

- インターネットに公開されているサーバに加えて、従業員の使用する端末のリスク、脆弱性を把握、管理
- これまでの資産管理ソフトによる端末のパッチ管理に加えて、CREMでインストールされているアプリケーションの脆弱性も実施
- 「スコア」化によりリスクを客観化することで、セキュリティ部門と事業部門でリスクの重要度を共有、迅速な対応が可能に

お客さまの課題

タニタでは従来のエンドポイント対策による不正プログラム対策に加えて、EDR、MDRの導入により、ランサムウェアなど、万が一に備えて最新の脅威が侵入した際の早期検知、対応を行っていた。「SaaS、クラウドなど組織の境界線を超えた利用が増える中で、エンドポイントにおける変化を把握し、対応する必要があった」と、株式会社タニタ情報システム部課長代理の宮澤裕之 氏はEDRを導入した背景を語る。ここで柔軟なSaaS、クラウド活用を進めるタニタでは、万が一攻撃を受けてしまった際の対策としてのEDRに加えて、攻撃につながる可能性のある脆弱性の可視化、管理の必要性を感じていた。Webサーバなどインターネットに公開されているリソースについては、定期的に脆弱性をチェックするサービスの存在も知っていた。ただこれらのサービスで得られる結果はある時点の一時的な状態に過ぎず、システムの変化を継続的に捉え、迅速に対応するには不十分であることに宮澤 氏は気づいていた。また、社内のクライアントやサーバについては、資産ツールを利用してOSのアップデート状況の確認などを行っていたが、脆弱性、特にインストールされているアプリケーションの脆弱性の可視化、把握までは行えない点に課題を感じていた。

選定理由

ここでタニタの検討に上がったのが、Cyber Risk Exposure Management（CREM）だった。CREMでは公開されている資産とその脆弱性を可視化するとともに、社員の利用するクライアントなど、社内の資産についても脆弱性に代表されるリスクの可視化を可能にしている。さらに資産の状態を継続的に把握、ダッシュボードとして提供するため、年数回に限定される一時的なセキュリティチェックではなく継続的なセキュリティ状態の把握が可能だ。「公開資産だけでなく、社内の資産も含め、継続的に脆弱性などの状況が把握できる点は、当社の求めていた対策像に合致していました」（宮澤 氏）さらに脆弱性が検知された端末やサーバは、その深刻度に応じてCREMでスコア付けされる。たとえ複数の端末やサーバで脆弱性が検知された場合であっても、スコアを参考に、重要度の高い資産から対応を進めることが可能である。このように機能としても求めていた対策に合致していたCREMであるが、その導入を後押ししたのは、会社としてのタニタのセキュリティ意識の高さであった。ランサムウェアなど、近年国内外企業が被害に遭う状況に対して、同社経営層は侵入後の対策に加えて、より強靭なセキュリティ体制の構築が必須だと考えていた。この実現には攻撃の侵入経路となりうる管理外の資産や脆弱性を可視化し、侵入が試みられる前に予防することが不可欠であると結論づけ、EDR、MDRに加えて、サイバーリスクの可視化、把握のためのCREM早期導入に踏み切ったのである。さらに「全てを自社リソースで実現することが難しい中、トレンドマイクロと連携してMDRを提供するパートナーの盤石な運用体制も採用の決め手となった」として、パートナーの存在を高く評価している。

ソリューション

タニタでは日本国内オフィスのクライアント、オンプレミスサーバ、クラウド環境のサーバ、工場の従業員端末を含めた700台超の端末にEDRを導入。MDRで常時監視、一元管理するとともに、CREMによりリスクを監視している。サイバーリスクの監視については、OSだけでなくWebブラウザなど端末にインストールされているアプリケーションの脆弱性も監視、管理するとともに、セキュリティ対策が弱い端末が侵入口となることがないように、導入されているEDRの機能の有効/無効も監視している。また公開資産のリスク管理については、国内に加えて海外現地法人の利用している公開ドメイン、Webサーバも対象にサイバーリスクの監視を行っている。

今後の展望

「EDR、CREMのいずれも、新型コロナウイルス感染症拡大以降、ゼロトラストという意識で導入したものです」とは、端末、サーバの最新の状態を把握するにとどまらず、その先を見据えた宮澤 氏の言葉である。タニタではEDRやCREMによるリスクの可視化に加え、他のセキュリティ対策と連携することで、ゼロトラストなどのアーキテクチャ、仕組みにつながることを期待している。

導入効果

「CREMの運用開始以降、脆弱性のあるサーバを特定し、適切に対策することができた」と宮澤 氏は運用開始時から想定通りの効果が得られていると話す。さらにCREMによるサーバなどの脆弱性の「スコア化」について、セキュリティ研修やトレーニングを通じてもともとセキュリティ意識の高い当社社員にとっては「当該資産を管理する部門に対応を依頼する際にも、セキュリティベンダが提供するスコアは具体性があり、円滑に調整、対応が進められています」とその効果を強調する。また、サーバのリスク監視においては、本社の管理するサーバに加えて、国内グループ会社が管理する社内サーバを監視することで、把握できていなかった脆弱性を可視化。「担当部門と連携することで攻撃される可能性を低減できている」とこちらも具体的な効果が得られている。

サイバーセキュリティの取り組みを一歩先へ

株式会社タニタのような組織が、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