SUCCESS STORY

G7サミットの安全を守るために強靭なエンドポイントセキュリティを実現

近鉄情報システム株式会社 https://www.kintetsu-is.co.jp/

大阪府、日本 | IT | 169名 (2023年7月1日現在)

ソリューション:

TrendAI Vision One™ XDR for Endpoints、TrendAI Vision One™ Endpoint Security、TrendAI™ Service One Essentials for MXDR Endpoints and Workloads、TrendAI™ Premium Service for Enterprise

※Trend Micro XDR Endpoint Sensor、Trend Vision One - Endpoint Security™、Trend Micro Managed XDR™ Endpoints and Workloads、Trend Micro Premium Support for Enterprise™は、それぞれ、TrendAI Vision One™ XDR for Endpoints 、TrendAI Vision One™ Endpoint Security 、TrendAI™ Service One Essentials for MXDR Endpoints and Workloads、TrendAI™ Premium Service for Enterpriseに製品名が変更になりました。

導入の背景

近鉄グループの一員として、近鉄グループホールディングス株式会社(以下、近鉄グループホールディングス)や近畿日本鉄道株式会社(以下、近畿日本鉄道)を中心にグループ各社の情報システムの企画、開発、運用などを支援する近鉄情報システム株式会社(以下、近鉄情報システム)。同社は現在、近鉄グループが推し進めるDX施策を支援しており、2023年10月にはそれまでホストコンピュータ上で運用してきた特急座席予約システムをAWSのクラウド環境に移行するなど、業界に先駆けて先進的なテクノロジーを積極的に導入・活用している。

グループ全体の情報セキュリティ対策については従来から実施していたが、2016年5月に三重県で開催された「G7伊勢志摩サミット(第42回先進国首脳会議)」を契機に、より一層のセキュリティ対策の強化を図るようになったという。

「G7伊勢志摩サミットでは近鉄グループが運営する施設が利用されたため、関係機関からセキュリティ対策に万全を期すよう要請がありました。そこで2015年に、それまで長年使い続けてきたトレンドマイクロのEPP(Endpoint Protection Platform)製品『ウイルスバスター コーポレートエディション』に加えて、インシデント対応の強化を目的にプレミアムサービスを新たに追加してエンドポイントセキュリティ対策の強化を図りました」

こう語るのは、近鉄情報システム 技術管理部長 中井昌樹 氏。担当エンジニアが付くプレミアムサービスの導入によりインシデント対応の体制がより強化されたことで、インシデント調査のリクエストから対応までのスピードアップが実現したという。

「長年トレンドマイクロ製品を利用していたので、EDR製品導入時の当社の変更要望に対して、担当エンジニアや営業の方からも開発部門へ強く働きかけしていただきました」

中井 昌樹 氏
技術管理部長

導入効果:

- EDR(Endpoint Detection and Response)の導入により出入口対策をすり抜けた脅威を素早く検知
- SOCサービスの利用により最小限の負荷でEDRを運用可能に
- プレミアムサービスの利用でインシデント対応力を強化

お客さまの課題

これらの対策強化により2016年のG7伊勢志摩サミットは無事に終了し、その後も特に大きなサイバー攻撃の被害に遭うこともなかったが、2023年6月に再び同じ地で「G7三重・伊勢志摩交通大臣会合」が開催されることになった。

前回のG7伊勢志摩サミットからの7年間で、ランサムウェアなどのサイバー攻撃の脅威はより高まっており、あらためて最新のセキュリティ事情にマッチした対策の在り方を検討することになった。

中井 氏によれば、その際に真っ先に課題として挙がったのが「エンドポイントセキュリティ対策」だったという。

「いわゆる『入口対策』『出口対策』についてはすでにある程度強化していましたが、コロナ禍に各社でテレワーク環境を整備したことを考慮し、すり抜けてしまう可能性が高くなってきていると考え、脅威が内部に侵入することを前提とした対策が必要だと感じていました」

そこで白羽の矢が立ったのが、「EDR」だった。EDRはエンドポイント端末の状態を常時監視し、未知の脅威や攻撃の予兆を素早く検知できるため、近年被害が続出しているゼロデイ攻撃やランサムウェア、潜伏型のマルウェアなどにも効果的に対処できると判断した。

「トレンドマイクロのEDR製品は攻撃を検知するだけでなく、それをブロックするためのパターンファイルも素早く作成・提供されてEPP製品に反映されるので、インシデントを確実に収束させることができます」

長尾 礼司 氏
技術管理部

「EDRを使った日々の監視は基本的にトレンドマイクロのSOCサービスにお任せしているので、弊社側の運用業務に掛かる負荷はほとんど増えていません」

矢後 友也 氏
技術管理部

選定理由

早速同社は主だったセキュリティベンダー各社のEDR製品を複数ピックアップし、ベンダーからのヒアリングやそれぞれの機能を比較検討した上で選定候補製品を絞り込み、さらに構築した評価環境において各製品やSOCサービスについて具体的な検証を実施した。その結果、最終的に同社が選んだのがトレンドマイクロのEDR製品、TrendAI Vision One™ XDR for Endpointsと、その運用・監視をトレンドマイクロが代行するSOCサービス、TrendAI™ Service One Essentials for MXDR Endpoints and Workloadsだった。

さらにEPP製品もこれまでのオンプレミス型のものからSaaS型に切り替えて、トレンドマイクロの TrendAI Vision One™ Endpoint Securityを採用し、プレミアムサービスに関しても引き続き契約することにした。

エンドポイントセキュリティ対策に必要な製品・サービスをトレンドマイクロ製品で統一した理由について、近鉄情報システム 技術管理部 長尾礼司 氏は「実効性のあるセキュリティ対策を実現するには、単体の製品・サービスが優れているだけではダメで、出入口対策から内部対策、SOCサービス、さらにはインシデント対応支援に至るまでの一連の対策が連動している必要があります。その点トレンドマイクロの製品・サービスは、脅威の検知から対応、インシデントの終息までの一通りを一括してお任せできると考えました」と説明する。

また近鉄情報システム 技術管理部 矢後友也 氏によれば、TrendAI Vision One™ XDR for EndpointsとTrendAI™ Service One Essentials for MXDR Endpoints and Workloadsは他社の製品・サービスより当社の運用環境に適していると感じたという。

「一定期間、評価環境に各製品とサービスを導入して、ホワイトハッカーの協力を得ながら実戦さながらの攻撃をいろいろ仕掛けてみましたが、TrendAI Vision One™ XDR for Endpointsは他社製品が検知できない攻撃でも検知できました。また他社のSOCサービスでは脅威を検知しても通知する基準に満たないということで連絡がないこともあったのですが、 TrendAI™ Service One Essentials for MXDR Endpoints and Workloadsはそのようなことは一切なく、連絡が来ました」

ソリューション

こうして同社はトレンドマイクロのエンドポイントセキュリティ製品・サービス群を選定、近鉄グループホールディングスが導入を正式に決定。半年間という短い期間で製品・サービスの導入だけでなく社内における運用プロセス設計も含めて、すべての導入作業を会合までに万全の準備を備えることができた。その過程においては、同社の要望が製品の仕様に新たに追加されたものもあったという。

「トレンドマイクロのSOCで緊急性の高い脅威が検知された際には、即座に該当端末をネットワークから隔離しています。その際にユーザ側に隔離されたことを通知する機能の追加をお願いしたところ、短期間のうちに製品の正式機能として実装していただきました」(長尾 氏)

こうして2023年3月、EDRを含む新たなエンドポイントセキュリティの本番運用がスタートした。幸いにもその後は現在に至るまで、深刻な脅威が検知されたことはない。しかし、特定のアプリケーションや意図的にイレギュラーなシステム操作を行った際にはSOC担当者からすぐに異常検知の連絡を受けており、「本当のインシデントが発生した際にも検知して素早く連絡してくれる」という安心感が得られているという。

今後の展望

なお同社は今後、重要インフラ事業者(近畿日本鉄道)として来るべき大阪万博に備えるためにも、さらに強固な環境作りを目指していくとしている。これまで強化してきたエンドポイント対策に加えてSIEM製品を新たに導入し、広範な脅威の可視化・検知能力の強化を進めていく計画もあるという。加えて今後は業務システムのクラウド移行を進める方針であることから、クラウドセキュリティの強化も進めていくとしている。

これらの将来構想を実現する上でも、トレンドマイクロの製品・サービスの進化には今後も大きな期待を寄せていると矢後 氏は話す。

「クラウドの利用拡大にはセキュリティの強化も不可欠で、仮想パッチを使ってサーバの脆弱性を保護するTrendAI™ Deep Security™ はその特効薬のような存在でした。当社では今後も積極的にクラウドの利活用を進めて行く計画もあるので、効果的にクラウド環境を保護できて使い勝手のよい製品が提供されてくることを期待しています」

サイバーセキュリティの取り組みを一歩先へ

近鉄情報システム株式会社のような組織が、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

Copyright ©2026 Trend Micro Incorporated. All rights reserved. [Kintetsu_Success_Story_20240301JP]
TrendMicro.com