TrendAI™

NICE WORK
OKUMURA

SUCCESS STORY

EDR、攻撃対象領域の可視化、優先度に基づく脆弱性対応で、24×365で稼働する現場の端末も、組織の“ナイスコミュニケーション”も守る予防型セキュリティ。

奥村組土木興業株式会社 https://www.okumuradbk.co.jp/
大阪府、日本 | 総合建設業 | 935人

ソリューション:
CREM (Cyber Risk Exposure Management) あんしん
プラス ウイルスバスタービジネスセキュリティサービスあんしんプラス
ウイルスバスタービジネスセキュリティサービスあんしんプラス Managed EDR Option

導入の背景

「土木·建築工事」「ガス工事·舗装復旧工事」「建設資材の製造販売·リサイクル」の3つの領域で事業を展開する奥村組土木興業株式会社。日本各地の道路·トンネル·河川·港湾などの社会基盤づくりにも携わる同社では、「良い仕事は良いコミュニケーションから」と経営本部情報システム室室長の桑名 氏が語るとおり、「ナイスワーク·ナイスコミュニケーション」を経営理念に掲げ、遠隔地の現場に年単位で滞在する従業員とも、ITを活用して密接にコミュニケーションを取り、帰属意識の醸成、メンタル面でのサポートに留意している。

同社は、ガス会社や中央省庁など、多様な発注者からのセキュリティ要件を満たす必要があり、なおかつ多くの協力会社をサポートするために貸与端末の管理も行うなど、従来セキュリティに対する意識は高い。その同社でも、昨今の脅威の高度化、環境の複雑化、ネットワーク境界の曖昧化などにより、従来の境界型防御やEPPでは対応しきれないという危機感が高まり、「平時からのセキュリティ対策」を強化する必要性を実感。また、高度な脅威検知や脆弱性管理を同社内で完結することが難しいため、外部の専門家による監視とサポートを含むソリューションの導入が不可欠となった。

導入効果:

- 従来の境界型防御だけでは太刀打ちできない昨今の高度化·巧妙化する脅威も対策可能に
- 休日夜間も稼働する現場のある同社において、自社の情報システム室が対応できない時間に何かあったとしても、マネージドサービスにより外部の専門家に対応してもらえる安心感
- 端末の脆弱性などをリスクスコアで確認できるため、根拠が明確な優先度に沿って脆弱性対応が可能。目標数値も持つことも可能に

お客さまの課題

全国の土木·建築現場に仮設事務所を構える必要があるため、コロナ禍以降に多くの企業で一般的となったリモートワークを以前から行っていた奥村組土木興業。ただ、いつ誰が現場に出ていつ戻るか見通せず、休日夜間も勤務する現場もある中で、すべての端末の可視化、継続的監視、脆弱性対応に限界を感じていた。

当時使用していた他ベンダーのEPP製品では、エージェントの稼働率悪化、原因不明のアップデート不備による遠隔アンインストール·インストールの繰り返し等の課題があり、別の製品を模索していた。

そこに、取引先からのセキュリティ要件強化、SaaSの利用拡大などの環境複雑化、高度化·巧妙化するサイバー脅威といった要因も加わり、平時からのセキュリティ対策強化の必要性とともに、自社での監視体制構築や脆弱性対応の困難さから、外部専門家のサポートが得られるマネージドサービスの必要性も実感することとなった。

「今まではリスクを数値で見ることができず、勘や予測で脆弱性対応を行っていました。CREMでは具体的な数値として出てくるので、目標設定がしやすく、対策も打ちやすくなりました」

桑名 良宣 氏
経営本部 情報システム室 室長

「ICTを活用して社内のコミュニケーションを活発に行うためには、セキュリティを確保し、安心して使ってもらう必要があると考えています」

髙田 亮 氏
経営本部 情報システム室 情報システム課 課長

選定理由

奥村組土木興業では、ITを積極的に活用しDXを推進しているが、それを安全に進めるためにセキュリティは必須とみなしている。セキュリティ対策を「事業継続性と信頼性を守る経営課題」と位置づけ、新入社員は入社後の研修で情報セキュリティ教育を受講、また各従業員も年に1回のEラーニングによるセキュリティ教育も受けるなど、セキュリティ意識が深く根付いた社風である。同社ではトレンドマイクロのパートナー企業である日本事務器株式会社の「ウイルスバスタービジネスセキュリティサービス」を長年利用してきた。今回の「あんしんプラス」の導入においては、この既存環境をそのまま活かして移行負荷を抑えられる点、日本事務器による安定した運用実績、さらに、同社による監視・運用サポートに大きなメリットを感じた。また、トレンドマイクロのサイバーセキュリティ業界における長年の実績や、最新脅威に対応する技術力を評価している。具体的には、エンドポイント、ネットワーク、クラウド、メールなど、複数レイヤに対応する包括的なソリューションを提供している点に加え、ゼロトラストやクラウドセキュリティ、AIを活用した脅威検知など、最新のセキュリティ課題に迅速に対応できる点である。また、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™ 」に統合することで、複数のセキュリティ対策を1ベンダに集約でき、運用効率と可視性が向上する点も好感触。国内外の豊富な導入事例も後押しとなり、複数製品・サービスの中からの選択に至った。

ソリューション

「ウイルスバスタービジネスセキュリティサービスあんしんプラス」を全社に展開、1500台を超える端末へのEDR導入が実現し、万が一のインシデントにも早期に対応できる体制が整った。さらに、Managed EDR Optionで日本事務器による24時間365日の監視も行われ、高度な脅威の検知力が向上。「CREM(Cyber Risk Exposure Management)あんしんプラス」も1500台超の端末に導入。IT資産の可視化が実現するとともに、脆弱性監視、外部公開ドメインの継続的監視を実施。各端末の脆弱性と当該端末の組織における重要度を掛け合わせたリスクスコアと、それに基づく優先度にしたがって脆弱性対応を行うことにより、組織全体の攻撃リスクの低減と、低リスクの状態を維持できるようになった。

今後の展望

奥村組土木興業では、今後のセキュリティ対策として、取引先や委託先を含めたセキュリティ評価と監視体制の構築によるサプライチェーンリスクへの対策、SaaS利用の拡大に伴い、認証・認可を強化することによるゼロトラストの推進、Microsoft 365や外部公開システムを含め、統合的な防御を実現するクラウドセキュリティの高度化、AIを活用した脅威予測によって予測型セキュリティを推進し、攻撃を受ける前に対策を講じる仕組みの定着を挙げている。

それに伴い、トレンドマイクロに寄せる期待として、ゼロトラストやAIなどの先進的な技術の継続提供、組織のセキュリティ運用負荷軽減のためのマネージドサービスの強化、複数レイヤへの包括的なセキュリティを確保する統合プラットフォームの進化を挙げた。

導入効果

TrendAI Vision One™ の統合されたコンソール、ならびにCREMによって、全端末・主要ドメインの脆弱性状況を一元管理できるようになった結果、リスクの把握が容易になり、可視性が向上した。

EDRによるリアルタイム検知と、日本事務器の運用サポートにより、対応スピードが大幅に向上。「EDRを導入しても、的確かつタイムリーな運用を自社内で行うには限界がある」(経営本部情報システム室情報システム課 課長 髙田 氏)と判断し、マネージドサービスを選定したことに非常に価値があった。

また、CREMによる脆弱性診断と改善サイクルを継続的に組み込み、攻撃を受ける前に対策を講じる文化が浸透、予防型セキュリティ(プロアクティブセキュリティ)が定着した。「毎日胃の痛い思いをしていたところ、安心していられる。今までできていなかったプロセスを埋めることができた」と桑名 氏。

サイバーセキュリティの取り組みを一歩先へ

奥村組土木興業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