SCSK Minori ソリューションズ 株式会社

事後対応型の対策よりも 優先順位の高いEPPの強化を実現

EDRという事後対応型の対策より優先すべきEPPの強化を実現

フルスキャンによるPCへの負荷がなくなり業務への影響を軽減

クラウドへの移行により管理基盤のメンテナンスが不要に

会社紹介

Minoriソリューションズ、CSIソリューションズ、Winテクノロジが 2021 年に合併して生まれた SCSK Minori ソリューションズは、SCSKグループの一員として、「夢ある未来を、共に創る」という経営理念のもと、開発やクラウド、マイクロソフトテクノロジーといった強みを活かして変化に対応するソリューションを通して幅広い顧客を支援している。

導入の経緯

Minoriソリューションズ、CSIソリューションズ、Winテクノロジが 2021 年に合併して生まれた SCSK Minori ソリューションズは、アプリケーションの開発、マルチクラウド基盤のソリューション、マイクロソフト系ソリューションといった旧三社それぞれの強みを活かしながら、最適な IT サービスをワンストップで提供している。

コロナ禍を経てテレワーク環境が浸透し、クラウド活用の場面がいっそう広がった後、再びオフィス回帰が進みつつあるといった具合に、ビジネスを取り巻く環境は目まぐるしく変化した。その中で同社は、こうした変化に対応するソリューションを技術力や知見とともに提供し、顧客の事業成長に貢献してきた。

そうした立場から、セキュリティ順守に対する社内への定期的な啓蒙と、人への啓蒙だけでは補えない領域を AI や新しいテクノロジーで補うために日々意識を高めていた。「経営から言われるまでもなく、機密事項や個人情報の漏洩を防ぐことに常に注力しています。日々最新のセキュリティ動向を注視するほか、やはり最終的に守るのは『人』であることからセキュリティに関する啓蒙を定期的に行い、社員の意識向上に継続的に取り組んでいます」（SCSK Minori ソリューションズ　技術企画本部 情報システム部長　荷見誠氏）

そのような同社は合併以来、基幹システムをはじめとする IT 基盤の統合に取り組んできた。PC を保護するエンドポイントセキュリティについても、以前は三社それぞれ別々のウイルス対策ソフトを導入していたが、そのままバラバラに運用していては負荷が高い上に、セキュリティ水準にもばらつきが出る恐れがある。「まず一番の課題として、セキュリティ製品の統合に取り組む必要があると認識していました」（荷見氏）

加えて近年、国内でもサイバー攻撃、特にランサムウェアの被害が激増している。「我々もそうした状況は耳にしており、やはり多様な脅威に備えてリスクを低減しなければならないと考えていました」（荷見氏）

選定のポイント

当初、SCSK Minori ソリューションズが新たなエンドポイントセキュリティ対策として検討したのは EDR 製品だった。当時、すでに導入していた製品に追加オプションの形で導入でき、国内での導入事例も増えていることから無難な選択肢に思えたが、情報収集を進めていくと、より優先すべきポイントがあることに気が付いたという。

きっかけはいろいろなソリューションを調査していく中で、社内から情報を得たディープラーニングによる高検知率、低誤検知率を誇る製品「Deep Instinct」と出会ったことだった。Deep Instinct のことは、それまで耳にしたことはなかったが、説明を聞き、まず優先して強化すべきは EPP だと考えるようになった。

「EDR はあくまで、インシデントが起こった後に検知する事後対応型です。いろいろな感染事例を見ていても、やはり EPP を強化し、マルウェアの攻撃を防ぐこと自体を優先すべきではないかと考えるようになりました」（荷見氏）
さらに実際に製品デモを見たことをきっかけに、メリットが見えてきた。
「まず、既存のウイルス対策製品に比べ、システムへの負荷がかなり軽減されていることを体感的に感じました」（荷見氏）。以前の製品はいずれも、定期的にフルスキャンを実施するたびに PC の負荷が高まり業務に影響が出る場面もあったが、それがなくなるのではないかと考えたのだ。

また、EPP の強化という本来の目的にとって最も重要な、脅威の検知力も優れていると判断した。「従来のパターンマッチング型ではなく、自律型で、ファイルの構造を解析してマルウェアかどうかを判断する仕組み自体、これまでとは比較にならないほど優秀だと、デモを見ただけでも感じました」（同社技術企画本部情報システム部　吉川諭氏）

導入の効果

こうした要因から SCSK Minori ソリューションズは Deep Instinct の導入を決定し、2023 年 9 月から社内への展開を開始した。まず情報システム部が属する技術企画本部内でインストールし、動作を確認した上で、全社約 2000 台の PC に展開するという具合に段階的に広げていった。

アラートのみを出力する検知モードで展開し、問題なく動作することが確認できた時点でブロックモードに切り替え、既存のアプリケーションの動作に影響を与えることなく導入を進めた。
「本当に大丈夫だろうかとビクビクしながら、少しずつ切り替えを進めようと考えていましたが、販売パートナーから提供いただいた導入シナリオのおかげで、切り替え後、ユーザーからの問い合わせはほとんどありませんでした」（吉川氏）

といっても同社の業務、特にアプリケーション開発業務は定型的なものではなく、さまざまな開発ツールや環境を活用している。このため、過検知に対する懸念は導入前からあった。

「現場では私も初めて見るような開発ツールや AWS をはじめとするクラウド開発関連のツールも使われています。展開当初はこれらが悪意あるものとして検知されることもありましたが、Deep Instinct のダッシュボードから詳細情報を確認したり、実際に使っているかどうかを当該ユーザーに確認したりして、その都度ホワイトリストに追加していきました」（吉川氏）

SCSK Minori ソリューションズ
技術企画本部 情報システム部長
荷見誠氏

このチューニング作業において有用だったのが、提供されたガイドだった。
「事前にレクチャーを受けたほか、過検知が生じた際にはどう対応すべきかのフローも用意していただき、ノウハウを共有してもらったため、問題なく進めることができました」（吉川氏）その後、数ヶ月運用を回していく中で、過検知の数は大幅に減ってきているという。
「むしろアラートが出ることで“きちんと止めてくれている”という安心感が得られています。何も音沙汰がないと、それはそれで本当に大丈夫かと不安になりますが、Deep Instinct ではエンドポイントの中で疑わしいものを逐一検知してくれます。それらを我々が判定し、許可していく一連のフローによって脅威の見える化ができています」（吉川氏）

以前のウイルス対策製品ではメール通知を確認するだけで、自ら管理コンソールをチェックすることはほとんどなかった。だが Deep Instinct 導入後は、ほぼ毎日のように確認しており、運用側のセキュリティ意識にもポジティブな効果があるという。

導入から今に至るまでインシデントは発生しておらず、以前のウイルス対策ソフトもアンインストールするに至った。ユーザーの細かい感想は、今後アンケートなどを通じて収集していく予定だが、「ユーザー視点ではあまり気づかないかもしれませんが、週に一回行っていたフルスキャンがなくなり、処理がその負荷に引っ張られる事態もなくなったのではないかと期待しています」（吉川氏）

特に、以前はウイルス対策ソフトでマルウェアを検知すると、PC を抜線してフルスキャンをするフローとしていたため、ユーザーはその間業務を止めざるを得なかった。これに対し Deep Instinct では、アラートが出た時点ですでに疑わしいプロセスは隔離されている状態となる。
「業務を止めることなく端末の調査ができるため、ユーザーの負荷も減り、時間の面でも大きなメリットがあると思います」（吉川氏）

その上、これまでオンプレミス環境で運用していたウイルス対策ソフトの管理基盤が、Deep Instinct のクラウドに移行することで不要になった。
「かなり昔に構築した古い基盤だったためメンテナンスの負荷も高く、どう更改するか悩んでいましたが、それもきれいさっぱり捨てることができました」（吉川氏）

今後の展望

「EDR も大事ですが、優先順位を考えるとまず EPP の強化であり、それができた後にあらためて進めていくべきではないかと思います」（荷見氏）という方針のもと、Deep Instinct を導入した SCSK Minori ソリューションズでは、Deep Instinct の運用を同じ部内の運用部隊に移行させつつ、新たな脅威に備え、引き続き対策を模索していくという。

Deep Instinct によってリスクを大きく減らせたのは事実だが、これで 100%万全というわけではなく、多層的な防御が必要だと考えている。
「万一感染してしまえば大きなダメージが生じます。だからこそ、事業継続のリスクを限りなくゼロに近づけるために、次にどういった手を打つべきか検討していかなければならないと考えています」（荷見氏）具体的には、あらためて EDR や MDR の導入を検討して万一侵入された場合の策も講じ、Deep Instinct との相乗効果を高めていく方針だ。

同時に、こうした経験を通して得られたナレッジを、顧客へのソリューション提供にも生かしていく。
「PC 入れ替えのプロジェクトにおいても、近年はセキュリティについてどのように考えているかを重点的に見るお客様が増えています。Deep Instinct はもともと他製品からスムーズに乗り換えできるという利点がありますが、自社で全社的に導入したノウハウを活かしながら提案を進めていきたいと思います」（同社クラウド基盤ビジネスユニット　クラウド基盤サービス第二事業本部　MS 事業サービス部　第二課　波多野公則氏）

情報システム部も「我々はただのバックヤード部隊ではなく、現業ビジネスに貢献していくことも役割の一つだと考えています」（荷見氏）という認識のもと、自らの経験やノウハウを活かし、セキュリティも含めた PC の運用管理など、顧客の情報システム運用を包括的に支援するサービスをさらに拡大していく予定だ。

「EDR はあくまで事後対応型です。やはり EPP を強化し、マルウェアの攻撃を未然に防ぐこと自体を優先すべきではないかと考えるようになりました」

SCSK Minori ソリューションズ　技術企画本部 情報システム部長　荷見誠氏