DARKTRACE

ケース スタディ

INAP Japan 様

概要

業界

- ネットワーク関連サービス

課題

- 事業規模の拡大に伴い、自社のセキュリティ対策を効率的に改善・強化
- ISP 事業者として、顧客のミッションクリティカルなネットワークを保護する必要性
- 既存のセキュリティ製品導入時に要したルール設定にかかる時間や負荷を軽減

結果

- 外部からのマルウェアの挙動だけではなく、コンプライアンス違反につながる疑わしい内部の通信もリアルタイムに可視化
- 面倒な事前設計やチューニングが不要で、脅威検知の自動化によって生まれるエンジニアのリソースで生産性を向上
- 日本国内で増加し続ける内部脅威による情報漏えいを未然に防ぐために最適な製品として、顧客に Enterprise Immune System の再販を提案

ビジネスの背景

INAP Japan (以下 INAP) は、2001 年に米国 INAP 社と日本の NTT グループとの合弁により設立された企業で、ISP 事業者として培った独自のネットワーク技術「インテリジェント・ルーティング」を活かし、FX や E コマース、データセンタ、クラウド事業者など、インターネット上でミッションクリティカルな業務を行う企業に対して高品質なインターネット接続サービスを提供しています。また、英語・中国語にも対応する海外向けカスタマーサポートやコールセンター業務を年中無休で代行するバイリンガルITサポートも絶大な支持を得ています。

> 企業規模が今後大きくスケールしても、事前設計やチューニングが不要で、ネットワークを止めることなくアプライアンスが自動学習し続けてくれるので、煩わしさや不安を一切感じません。
>
> **INAP Japan 技術部長 吉川 進滋 様**

課題

INAP は現在、従業員数約 30 名で法人向けインターネット接続サービス、バイリンガル IT サポート等を展開していますが、お客様の数が増加するにつれて同社の社員を増やす必要が出てきました。ISP 事業者として社内のエンジニアの割合が高いことから、30 名規模のオフィスでは社員がデバイスを使って普段何をしているか、オフィス内を見渡すことで概ね把握できますが、将来 100 名～200 名規模に拡大すると、当然デバイスの数も増えて、現体制のままで全社員の行動や通信パターンを把握することが難しくなるため、新しいセキュリティ対策を講じる必要が出てきました。

一方で、お客様に対するネットワークセキュリティサービスとして、INAP は 24 時間 365 日体制のサポートを展開しており、主にファイアウォールや IDS/IPS 製品を活用してお客様のネットワーク環境を監視・運用するフルマネージドサービスを提供しています。しかし、既存のセキュリティ製品ではルールの定義やテストをするために数か月を要することもあり、同社のサービス導入企業が増え続ける中、限られた人員でより効率的なセキュリティ運用を進めることは喫緊の課題でした。

解決策

日々進化する外部脅威やゼロデイの脆弱性、内部脅威などのセキュリティリスクが増大する一方で、業務の効率性を著しく損なうような過剰なセキュリティ対策は望ましくありません。利便性とセキュリティ強度の両立がうまくできるような効率的なセキュリティ対策を取り入れたいと考えていたとき、導入が容易な上に成果が大きいDarktraceのEnterprise Immune Systemに出会いました。

INAPはPoV（※）の期間中、社員の個人PCを一時的にネットワークに接続して、本来は業務中に使用すべきではないファイル共有ソフトやインターネットの接続経路を匿名化するツールを試しにインストールしてみたところ、Enterprise Immune Systemがほぼリアルタイムにこれを異常として検知したことを確認しました。これらのP2P接続を悪用すると、数メガのテキストデータでしかない個人情報は数分もあれば漏えいするリスクがありますが、Enterprise Immune Systemはインストールした直後にリアルタイムに異常な通信として可視化することに成功しました。

> 最近、日本国内で発生した重大なセキュリティインシデントを振り返っても、外部からの攻撃よりも悪意のある内部関係者による情報漏えいの方が被害は甚大です。疑わしい内部の挙動をリアルタイムに検知、可視化するEnterprise Immune Systemを導入することは、極めて大きな抑止力につながります。
>
> INAP Japan
> **技術部長 吉川 進滋 様**

利点

人手でログや通信フローから目視で異常を検知しようとすると、管理者に非常に高いスキルが求められるだけでなく、それにかかる労力や時間が膨大となるため、プロアクティブな内部ネットワークの監視はこれまでは現実的な運用ではありませんでした。しかし、Enterprise Immune Systemを導入すれば、ネットワーク内部の通信の異常をAIが的確に検知することで、経験が少ないエンジニアでも効果の高いセキュリティ運用を無理なく実施することができます。これを自社の事業規模の拡大を図るフェーズで導入したことで、未知の脅威や内部不正に対応しつつエンジニアのリソースを他の生産的な業務に充てることができます。さらに、Eコマース事業者のように膨大な個人情報を保持する既存のお客様に対して、再販の提案も進めやすくなりました。

（※）4週間の導入前検証。

お問い合わせ

Tokyo: +81 3 5456 5537
North America: +1 415 229 9100
Europe: +44 (0) 1223 394 100

japan@darktrace.com
darktrace.jp