DARKTRACE

ケース スタディ

日本テレマティーク株式会社様

日本テレマティーク株式会社

概要

業界

- 情報通信サービス

課題

- 情報システムの開発・販売活動を軸に ICT 事業を展開する企業として、情報セキュリティは事業活動の最重点事項
- サンドボックスや IPS、IDS 製品、一般的なエンドポイント防御によるシグネチャベースの脅威検知の限界
- 既存の製品では、改ざんの予兆や不正が疑われる通信の有無などの逐一監視は困難

結果

- 人為的なセキュリティポリシーやコンプライアンス違反を疑う行為の検知
- 新たな脅威の時代における情報セキュリティに対する感性のレベルアップ
- システム運用保守サービス、コンサルティングの付加価値向上

ビジネスの背景

日本テレマティーク株式会社（以下 NTI）は、情報通信ネットワークサービスに関わる技術に優れた NTT 東日本と、グローバルなビジネスチャネルを有しサービスや製品の評価能力に長けた伊藤忠商事を株主に持ち、1985 年に設立されました。CRM システム、コールセンター構築、ネットワークシステム構築や仮想化ソリューションに強みを発揮する ICT カンパニーです。

> Darktraceはこれらのシステム運用保守サービスと親和性が高いと認識しており、まずは自社で Enterprise Immune System を使いこなして製品の理解や知見を蓄えた上で、TIR（※1）も含めて今後お客様にサービスとして積極的に提供していく予定です。脅威となりうる兆候を学習・発見し、更に原因を解決すると共に、お客様のシステムの今後の姿を提案・実施することにより、付加価値の高いコンサルティングにつなげたいと考えています。

日本テレマティーク株式会社
システムソリューション事業本部
システムコンサルティング部 岩波 久善 氏

課題

システムインテグレーターとして、お客様の ICT システムの設計、構築、運用を事業の柱にしていますが、企業規模に鑑みて、お客様の幅広い情報通信システムへのニーズに対し総合的に対応することよりも、専門的な領域に特化したサービスをお客様に提供することをビジネスの主軸に据えています。

その中でも、情報セキュリティを最大の付加価値の一つとして位置付け、最先端のユニークなセキュリティ製品に対して高い関心を持ち続けてきました。先進的な製品を自らのシステム環境に導入して実践的に試行運用に取り組む企業文化の下、セキュアな環境構築を積極的に推進してきました。

自社でセキュリティポリシーを策定した上で、これまでにサンドボックスや IPS、IDS など様々な製品を導入してきましたが、社内のネットワーク環境がポリシーに則って運用されているかをこれらの製品群で逐一監視し続けるための人的リソースに限界を感じるようになりました。また、新たな脅威が次々と出現する中で、コンサルティング企業としての情報セキュリティに対する感性の底上げを図り、新たな対策を積極的に導入しながら、さらなるルール策定や情報共有を推進して、インシデントの発生を防止することに加え、万一インシデントが起きた際も迅速にエスカレーションの上、適切な措置を講じることができる体制作りを進めたいと考えていました。

(※) 写真左から　日本テレマティーク 中山氏、高橋氏、岩波氏、佐野氏、柴田氏、保坂氏、吉澤氏

解決策

2016 年、あるサンドボックス製品の導入・拡販を念頭に置き、これと比較できる製品を探す中で Darktrace の Enterprise Immune System に出会いました。PoV (※2) を実施した結果、サンドボックス製品とは異なるものだということを理解しましたが、TAP 経由でトラフィックをコピーし、内部ネットワークを確認することで異常な振る舞いを検知するという観点では、当初は同列カテゴリの認識でした。PoV で検証した結果、サンドボックスや IPS、IDS などの製品は既存のシグネチャで定義されている攻撃には対処することを前提としていることに対し、これらの製品がいずれも検知できなかった人為的なセキュリティ違反の兆候を、Darktrace は自動的に検知することができました。

> 仮に例として、ポリシーに違反して Dropbox や Google Drive などを社員が使用していたとしても、従来のサンドボックス製品は、あくまでもユーザーの行為なので正常だと認識してしまいます。このような人為的な違反はネットワークの定常状態を自己学習する Darktrace の AI だけがリアルタイムに検知できるので、これは大きな優位性だと思います。
>
> **日本テレマティーク株式会社**
> **システムソリューション事業本部**
> **システムエンジニアリング部 保坂泰彦 氏**

NTI のネットワーク環境では、情報漏えいにつながるような深刻な脅威はこれまでに見つかっていませんが、Enterprise Immune System を運用する中で見つけられた有益な事象として、ファイルサーバへの夜間帯のアクセス状況、外部サイトへの暗号化されていない FTP 接続、普段あまりアクセスしない海外サイトへのアクセス状況、そこからのファイルのダウンロード状況などをリアルタイムに把握することができました。導入済みの個々のシステムのログを見れば、いずれも確認できる事象ですが、通常業務に並行して膨大なログの中から探し出して把握するというのは非常に煩雑です。機械学習によりネットワーク内部の通信パケットを分析し、そのネットワーク固有の通信パターンを常に自己学習して機能高度化を図る Enterprise Immune System ならではの特徴は、これらの兆候をリアルタイムに発見・可視化することが可能となり、運用上大変有益と言えます。

利点

Darktrace を導入したことで、未知の攻撃による不審な挙動の発見のみならず、内部不正やコンプライアンス違反の発見も可能とする能力を得られました。また、内部ネットワークの挙動を可視化することで、脅威となりうる事象を社内で共有しながら、従業員の情報セキュリティに対するルールの遵守はもちろん、未知の脅威への備えに対する感性も日々向上させています。

NTI では、事業の大きな強みとして NTI サポートセンタ (NSC) があり、お客様の ICT システムに対して 24 時間 365 日体制でリモート監視、インシデント対応、脆弱性対応、定期レポートなどをサービス提供しています。

(※1) Threat Intelligence Report：Enterprise Immune System が検知した異常や脅威を解析・評価し、対策をレポートするサービス。
(※2) Proof of Value：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