名村情報システム株式会社 様

1911 年、大阪で創業された名村造船所は、これまで数多くの船舶を世に送り出し、その評価は世界で定着しています。橋梁や沿岸施設などの大型鉄構造物も商品化しています。名村造船所の 100 年以上にわたる総合産業としての人材・技術・設備力を受け継ぎ、1983 年に分社・独立を果たした名村情報システムは、親会社である名村造船所のシステム開発・運用・保守を担い、制御系・事務処理系の開発や 28 年を超える金融系の情報システム開発・基盤構築など、多彩な分野で高い評価と厚い信頼を培ってきました。

まとめ

- ✔ 従来の出入口対策・境界型防御製品をすり抜ける脅威の増加
- ✔ セキュリティ運用を内製化してリアルタイムに近い脅威対処を低コストで実現したい
- ✔ あらゆる脅威を自律的に検知・可視化・調査分析する自己学習型 AI の導入により、漏れのない自社運用を少人数で実現

境界型防御の限界と高コストな SOC 運用

名村造船所では、従来のサイバーセキュリティ対策として、アンチウイルスソフトによるエンドポイント防御や、メールフィルタリングツールやサンドボックス製品を活用した出入口対策を長年実施していました。しかし、近年になってエンドポイントにおける不審な挙動が発生時ではなく後追いで検知されるなどの事象が発生し、このようなルールやシグネチャに依存する既存のサイバー防御に限界を感じていました。また、これらの境界型防御製品による日々の運用や分析業務を SOC ベンダーに委託していたこともあり、運用コスト面や脅威対処のリアルタイム性にも課題を抱えていました。

名村造船所ではかねてから従業員に対するセキュリティ教育に重きを置いており、年 2 回程度、全社対象のペネトレーションテストを行い端末の脆弱性やユーザーの反応を定期的に確認していることもあり、セキュリティに対する意識は非常に高く、業務継続に支障をきたす恐れがある深刻なサイバー脅威や情報漏えいなどの被害は今までに発生していません。しかしながら、昨今日本国内でもますます急増するランサムウェア攻撃やそれに伴う実害のリスク、Emotet 等の標的型メール攻撃の増加や、働き方の変化に伴う内部脅威リスクの増加に照らしても、万一の場合に備え、これらのサイバー脅威に対してリアルタイムかつ漏れなく対処できるセキュリティ体制の構築は急務でした。従来のエンドポイント防御やサンドボックス製品による「不正侵入のパターンや挙動を検疫する」アプローチではなく、「いつもの通信パターンと異なる通信を検知する」アプローチであれば、未知の脅威や新手の攻撃に対しても網羅的に対処できるのではと考え、AI による独自の自己学習型アプローチを採用する Darktrace 製品の POV（※）を開始しました。

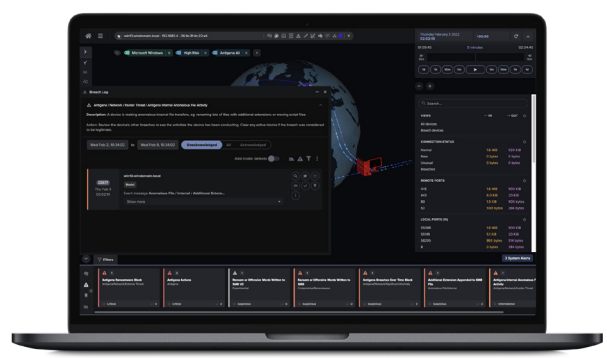
「評価導入時の選定ポイントは自社運用ができるかどうかでした。Darktrace 製品にはネットワークの普段の状態を機械学習する AI が搭載されているため、検知の抜け漏れや遅延がないという安心感と、通信異常の原因の調査分析まで人手を介さず自動化できる機能により、低コストかつ確実なセキュリティ体制を内製化することができました。」

名村情報システム株式会社 製造ビジネス本部 IT プラットフォーム部 宮地 俊明 様

AI によるリアルタイム かつ網羅的な対処

Darktrace Immune System の製品群は、人間の免疫システムに着想を得て独自開発された自己学習型 AI が、組織のネットワーク上のユーザー、デバイスの普段の挙動や通信パターンを自律的に機械学習・可視化し続けることで、定常状態とは異なる「異常」をリアルタイムに検知し、異常度に応じたアラートを発する仕組みを提供します。細かな事前設計やメンテナンスは不要で、ルールやシグネチャには一切依存せず、組織の「生活パターン」から逸脱する予兆レベルの脅威を AI が漏れなく自動的に検知・遮断・調査分析する唯一の製品です。パケットキャプチャにより Darktrace Immune System がアプライアンス内で解析する要素は、通信の宛先や時間帯、通信量・通信頻度などが含まれ、ユーザー毎、デバイス毎、サブネット毎にこれらの要素を継続的・自律的に機械学習することでネットワークの普段の状態のベースラインを更新し続けるため、理論上、いかなる未知の脅威や内部不正も検知・可視化することができます。オンプレミスの IT ネットワークに加えて、各種モジュールやセンサーを追加インストールすることでクラウド /SaaS 環境、リモートワーク端末を含む組織のあらゆるデジタルインフラを全域にわたり網羅的に監視・自律防御できることも特徴です。

機械学習のメカニズムは、IT ネットワークのコアスイッチに接続したアプライアンス製品がポートミラーリングによって業務端末と各種サーバー間のあらゆる通信パケットのヘッダー情報の収集・解析を行うというシンプルなものです。Darktrace 製品との比較検討時、EDR 製品の導入も俎上に上がりましたが、各端末に個別導入する必要があるエージェント型製品は、課金面のコスト増や導入に要する時間、通常業務への影響がネックでした。一方で、Darktrace のアプライアンス製品をインストールするのに要した時間は 1 時間程度で、事前設定を特に要することなく自律的に機械学習を開始しました。ネットワーク上を流れる通信パケットは Darktrace 独自の 3D 可視化ツールである Threat Visualizer によってウェブブラウザ上で一元的かつリアルタイムに描画されます。名村造船所のネットワーク上のあらゆる端末情報を受動収集・管理・可視化し続けているため、境界の監視に終始していた従来の対策では不可能だった AD サーバーに対する認証情報の把握をパケットレベルで実現、Threat Visualizer 上で瞬時に可視化できるようになりました。これにより、ユーザー ID を軸にした行動の監視ができ、また特権昇格など攻撃の予兆が発生した万一の際にも誰が端末を操作していたのか容易に特定することができるため、内部不正の未然防止まで網羅できている実感があります。



Darktrace Immune System はルールやシグネチャに依存せず、事前設計やメンテナンスも不要ながら、いかなる未知の脅威や内部不正にも理論上、リアルタイムに自動対処できる唯一のサイバー AI 技術を提供します。

AI による脅威の自動調査・ 日本語自動レポートで運用省力化

現在、名村造船所では 1,400 台弱の業務デバイスを対象に、24 時間体制で合計 5 名の運用担当者で Darktrace Immune System を駆使したネットワーク監視を同社グループ内だけで完結させています。このようなセキュリティ運用の内製化・一元化には、Darktrace が 2019 年の製品アップデートで追加した機能である Cyber AI Analyst が大きな役割を果たしました。Cyber AI Analyst は、検知したアラートを人間のアナリストが人手で調査分析する際の数百万におよぶ思考パターンを数年間にわたり機械学習し続けた AI を駆使し、AI が脅威調査までも高速自動化する世界初の技術で、検知したアラートの因果関係を瞬時に文章化し、平易な日本語でインシデントレポートを自動生成します。ワンクリックで AI が自動生成したレポートを PDF で出力でき、日本語による純客観的なレポーティングまで自動化できる術を手に入れたことで、名村造船所ではセキュリティ専任の担当者でなくてもネットワーク上で優先対処が必要な事象とその原因を一瞬で把握できるようになり、他社製品のログ調査や Darktrace によるアラートの深掘調査を人手で行う頻度を減らしたことで大きな運用コスト削減を実現しました。

（※）Proof of Value：4 週間の導入前検証。

詳細については以下をご覧ください

- 無償トライアルを申し込む
- Immune System ホワイトペーパーを読む
- Darktrace の YouTube チャンネル