東新工業株式会社 様

東新工業株式会社（以下、東新工業）は、めっき業界においてフープ材の「部分めっき」で世界的技術レベルの水準を持ち、業界をリードしている企業です。スマートフォンをはじめ、DVD、液晶型テレビ、PC などの電子部品用接点材料にめっき加工を実施しています。特に、銅合金やステンレス素材からなるプレス加工前後のフープ材に部分めっきを行っています。2001 年に ISO14001、2002 年に ISO9001 を取得し、環境および品質管理の体制が確立されています。

東新工業株式会社

まとめ

- ✔ ビジネス拡大に伴い新たに採用した業務端末・従業員を効率的に保護したい
- ✔ 能動的にログ分析する必要があるルールベースのセキュリティ製品を活用しきれない
- ✔ 自己学習型 AI 技術が通信異常に対して自動的に優先順位をつけて漏れなく対処してくれている安心感

境界型防御の限界と人材不足

神奈川県横浜市に本社を置く東新工業は、スマートフォンや PC 向けのマイクロコネクターのめっき加工でビジネスを急拡大しています。大手スマホメーカー等の主要顧客からの大量受注に迅速に対応するため、新たに 2019 年 10 月に松本工場（長野県）、2020 年 7 月にいわき四倉工場（福島県）をそれぞれ竣工し、既存のいわき好間工場（福島県）も含めて、現在国内に 4 拠点、海外に 2 社の合弁会社を展開しています。工場新設に伴い従業員数は急増、同時に業務に利用する PC の台数も倍増し、セキュリティ対策の強化・効率化は急務でした。従来からアンチウイルスソフトなどのエンドポイント製品を各 PC に導入していますが、外部からの不審な通信を本当に境界で全て検知できているのか、不安を感じさせるような軽微な異常も増加傾向にありました。

東新工業では、拡大を続ける同社のネットワークの運用管理の見える化・効率化を図るため、企業内 LAN に最先端の SDN（Software-Defined Networking）ソリューションを導入しており、ネットワークの仮想化・安定化を実現しつつ、内部の通信を監視する体制が従前から整えられていますが、セグメント毎にポリシーを設定した上でネットワーク監視・脅威制御を行うという SDN の性質上、予期せぬ未知の脅威には対処しきれない状況で、かつ万一の障害発生時に膨大なログデータを収集・分析するための人材や時間が不足していました。業務端末やユーザーの増加に比例してアタックサーフェスが拡大する一方、セキュリティ対策に割ける人的リソースには限りがあり、各端末にエージェント型の境界型防御製品を個別に追加導入・運用する出入口対策だけに終始するのは、コスト的にも、未知の攻撃や内部脅威に漏れなく早期に対処したいというニーズに照らしても現実的ではありませんでした。この恒常的な人材不足と増加の一途を辿るサイバーリスクへの対策を AI による自動化で一挙に解決できそうなセキュリティ製品を探す中で、Darktrace Immune System に出会いました。

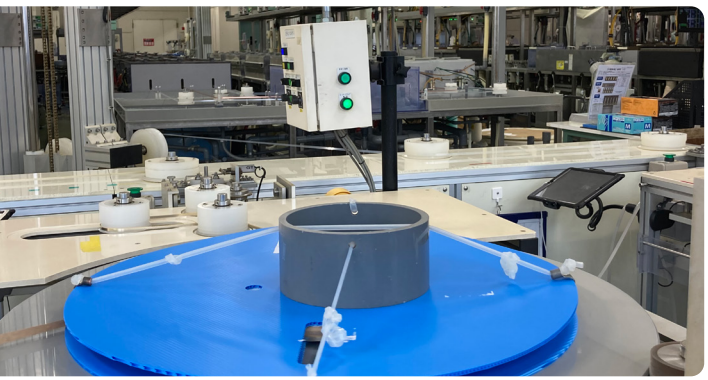
「増え続ける業務端末に個別にインストールする手間なく、境界をすり抜けてくる脅威や内部不正を早期に漏れなく検知できる自己学習型 AI により、安心感が飛躍的に高まりました。」

東新工業株式会社 総務部 横浜総務課 小松 隆 様

予兆レベルの脅威に自動対処

Darktrace Immune System 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内外のユーザー、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、異常度に応じてアラートを発する仕組みを提供し、ルールやシグネチャに一切依存せず AI が予兆レベルの脅威を漏れなく自動的に検知・遮断・分析できる唯一の製品です。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かつ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。

東新工業では、現在横浜市の本社・工場で使用する約 180 台の業務端末（PC、タブレット端末、プリンタ等）を監視対象として Darktrace 製品を導入・運用しています。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、業容拡大に伴い、製品導入前後で端末数は倍増したものの、アプライアンスのインストール作業に要したのは 1 時間程度でした。POV（※）の成果として、業務に関係しない海外製のアプリケーションを業務用 PC にインストールして利用を続けるユーザーの存在、東新工業で滅多に扱うことがない数ギガバイトにおよぶ容量の企業紹介動画データを外部のベンダーに送信する人事担当者の存在などが即座に明るみに出ました。前者に関しては別途導入済みの資産管理ツールのログを能動的に辿れば発見できる事象ですが、異常を自動的・受動的にアラートとして知らせてくれる自己学習型 AI の導入により、ピンポイントに把握したい異常のみを調査工数をかけずに把握する術を手に入れたことで、当初抱えていた人材不足や検知漏れに対する不安の双方の課題解決につながっています。

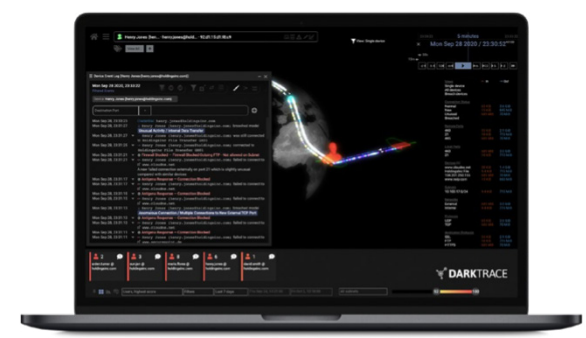


東新工業のネットワーク内部を流れる通信パケットは Darktrace 独自の 3D 可視化ツールである Threat Visualizer によってウェブブラウザ上で一元的かつリアルタイムに描画され、アウトバウンド / インバウンド、内部の横方向の通信も含めて漏れなく直観的に監視することが可能です。さらに、Darktrace Immune System が検知した異常は、定常状態からの逸脱度を客観的に示すしきい値をベースに瞬時に対処の優先順位が付けられ、高異常度のアラートや接続は Threat Visualizer 上で自動的に色分けして表示されます。東新工業では、しきい値を 50% ～ 100% のレンジに設定して日々運用しており、週平均 3 件程度のアラートが発せられる都度、原因となったユーザーに注意喚起を続けています。不正アクセスやマルウェアに起因するサイバー攻撃や内部からの情報漏えいなどの重大インシデントはこれまでに発生していませんが、自己学習型 AI により社内ネットワークの「生活パターン」が丸見えになることで、従業員のセキュリティ意識が確実に向上していることを実感しています。

（※）Proof of Value：4 週間の導入前検証。

「既存のセキュリティ製品や資産管理ツールのログを全部確認しようとすると 1 日数時間ほどかかります。一方、Darktrace Immune System は AI が異常のトリアージ・検知を自動化し、各アラートの原因調査まで AI が実施し、さらに日本語で調査結果を瞬時にまとめてくれるので、1 日 10 分ほどの工数で済みます。」

東新工業株式会社 総務部 横浜総務課 小松 隆 様



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