McLaren Group

1963 年、著名なレーシングドライバー Bruce McLaren 氏によって設立されたマクラーレンは、40 年以上にわたり自動車業界と F1 レーシングの最先端を切り開いてきました。年月を経てマクラーレンは単なるレーシングチームを超えて McLaren Racing、McLaren Automotive、McLaren Applied という 3 つの事業部を持つ企業に成長し、これらを保護する必要性に直面しています。

まとめ

- ✔ ダイナミックかつ分散したワークフォース
- ✔ 専用に作成された巧妙な E メール攻撃の標的となっている
- ✔ ビジネスの隅々までを保護するために AI を採用

「Darktrace は自律的にアクションを取ってくれるため、チームは作業から解放されハイレベルなタスクに専念できます。」

マクラーレン・レーシング、プリンシパルデジタルアーキテクト

進化する脅威環境に適応

世界最先端の知的財産の密かな盗み出しから数秒でデバイスを暗号化することができるマシンスピードの攻撃まで、サイバー攻撃はマクラーレンの勝敗を左右する問題になりかねません。 したがって、信頼のおけるパートナーや主要なサプライヤーとの間でしばしば共有される機密性が高いデータを保護することは最重要課題です。

マクラーレンのワークフォースはこれまでも常にきわめてダイナミックでした。チームは毎週末、世界のいろいろな場所でコースサイドにリモートオフィスをセットアップするに等しい作業に慣れていたのです。さらに、リモートワークへの広範な移行が Dropbox や Microsoft Teams などのクラウドや SaaS ツールへの組織の依存度をさらに高めました。Darktrace 導入以前は、こうした環境はサイロ型のポイントソリューションのばらばらな集まりで保護されており、これらのソリューションは事前に定義された悪意ある動作に頼って将来の脅威を見つけなければならないものでした。

そのため、セキュリティチームはビジネスの隅々までをカバーすることができる包括的で統一されたサイバーセキュリティプラットフォームを求めていました。クラウドおよび SaaS アプリケーションから E メールまで、マクラーレンは新種の脅威がどこに出現しようとも、それらを阻止できるソリューションを必要としていたのです。

自動対処

マクラーレンは自己学習型 AI を導入してルール、シグネチャ、あるいは事前の仮定をしようせずにリアルタイムに脅威を検知および調査することにしました。

Darktrace は組織のエコシステム内のあらゆるユーザーとデバイスの「生活パターン」の学習を即座に開始しました。「自己」とは何かを学習することにより、Darktrace の Immune System は SaaS アカウントの乗っ取りやデータ漏えいからゼロデイマルウェアや国家による攻撃に至るまで、サイバー脅威の兆候であるかすかな逸脱を検知することができます。

Darktrace の AI はオープンかつ拡張可能なアーキテクチャを通じて他のツールとシームレスに統合することができ、マクラーレンの既存のセキュリティスタックの価値を補強するとともにデジタルエコシステム全体に可視性を拡大しました。どこで攻撃が発生しようとも AI により自律的に撃退させることで、マクラーレンのセキュリティチームはすべてのアラートに対応する代わりに貴重な時間を週末のレースに集中させることができます。「テレメトリーを確認しない限りマシンをコースに送り出すことはできません。つまりこれは私達にとってクリティカルなインフラでありきわめて重要なのです。」マクラーレン・レーシングのプリンシパルデジタルアーキテクトであるエドワード・グリーン氏はこのように語っています。

「私達が通常どう振る舞っているかをこれほど短時間に AI に学習させることができるとは驚きでした。」

マクラーレン・レーシング、
プリンシパルデジタルアーキテクト

自己修復する受信箱

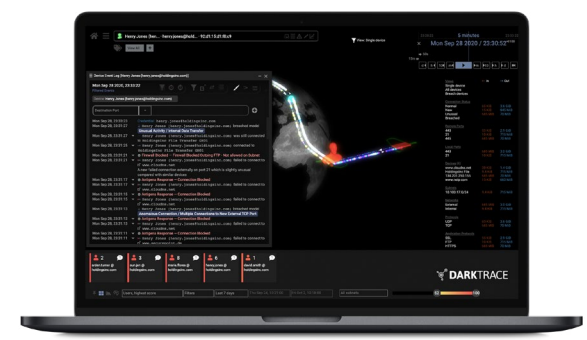
すべての組織同様、マクラーレンもソーシャルエンジニアリングからアカウント乗っ取りまで、さまざまな E メール脅威に直面しています。特に、最高責任者レベルのエグゼクティブを標的とした巧妙なスピアフィッシング攻撃についての心配を抱えていました。E メール攻撃の数が急激に増えるなか、マクラーレンは AI ベースのセキュリティシステムを Microsoft 365 システムの保護にも拡張し、Antigena Email を使ってワークフォースを悪意ある E メールから守ることにしました。

Antigena Email は自己学習型の AI によるアプローチを使ってあらゆる E メールユーザーのコミュニケーションのパターンを理解することにより攻撃のかすかな兆候を検知します。着信した E メールを事前定義済みのルールやシグネチャと比較して判定する代わりに、Darktrace は E メールをコンテキストに応じて分析し、新種の巧妙な攻撃を封じ込めると同時に、通常のビジネスは中断なく継続させることができます。

グリーン氏は次のように説明しています。「その効果は数日で確認できました。ユーザーから報告されるフィッシングメールの数は次第にそして大幅に減り、Antigena Email のアクションを定期的にレビューすることによってそれまで気づいていなかった数多くのフィッシング攻撃を発見するに至りました。」

「Darktrace は今年、我々人間が普通発見できないものを発見し、大いに自信を与えてくれました。」

マクラーレン・レーシング、プリンシパルデジタルアーキテクト



Darktrace の Threat Visualizer はクラウド、SaaS、E メール、コーポレートネットワーク内の脅威を表示します

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

E: japan@darktrace.com @darktracejp www.darktrace.jp