ランサムウェアから病院を保護

Cyber AI を使ってヘルスケア業界のセキュリティチームを補強および拡張

まとめ

- ✔ 世界で 280 以上のヘルスケア組織を保護
- ✔ 新種および巧妙な脅威を検知する自己学習型 AI テクノロジー
- ✔ 動きの速い攻撃を数秒で自律的に阻止
- ✔ トリアージまでの時間を 92% 短縮
- ✔ 業務の中断なし

Penn Highlands Healthcare
Swope Health Services
PHOENIX group
Carle
Northfield Hospital + Clinics
Life Group

ランサムウェアの急増：コンピュータースピードで展開されるサイバー攻撃に立ち向かう

病院や各種医療機関へのサイバー犯罪の拡大によりセキュリティチームは限界に達しつつあります。特にランサムウェアによる影響が大きく、パンデミックへの第一線の対応のサポートで既に疲弊し、過大な負荷がかかっているスタッフを狙って、デジタルシステムを中断させて身代金を得ようとしています。

昨年来、ヘルスケア業界を標的とした攻撃は倍増し、蔓延するこれらの脅威に対して FBI、CISA、HHS が警告を発しています。2020 年 3 月初めからの 1-2 週間だけを見ても、ランサムウェアはサンディエゴを拠点にした Scripps Health 社、アイルランドの政府機関である Health Service Executive、そしてニュージーランドのいくつかの病院を攻撃し、システムはオフラインに追い込まれました。 そして、この脅威はとどまることを知りません。

ヘルスケア組織にとってダウンタイムは到底許されません。サイバー犯罪者はこの事実を知っていて悪用します。 ランサムウェアに襲われた病院の現実は悲惨です。IT システムの停止により救急車のルート変更、急を要する手術の延期、治療オプションの縮小などにつながり、結果的に人間の生命を危険に晒します。

病院内のデジタルインフラはバックオフィスのネットワークや患者記録システムから、ネットワーク対応医療機器や IoT 装置に至るまで広範であり、重要なデータを保護してレジリエンスを構築する課題はかつてなく困難な課題です。

脅威についての数値データ

21
ランサムウェア攻撃による平均ダウンタイムは 21 日間

4000+
2016 年から 2020 年までの間のランサムウェア攻撃件数は 1 日 4000 件

$ 7.1 million
ヘルスケア業界でのデータ流出の平均コストは 710 万ドル

“ 自動対処技術は、動きが速く予測不能な脅威から被害を未然に防ぐ未来の形です。Darktrace が人間に代わって脅威を撃退してくれるため、私達は戦略的な取り組みに集中することができます。”

Milton Keynes Hospital、CTO、クレイグ・ヨーク氏

Cyber AI: マシンが脅威に対抗

世界中で 280 以上の医療機関に導入されている Darktrace の Cyber AI はランサムウェアのような動きの速い攻撃からの防御に対するデファクトテクノロジーとなっています。

Cyber AI は、組織内のあらゆるユーザーおよびデバイス、およびデジタル環境についての「正常」についての変化する理解を構築することで機能する自己学習型テクノロジーです。 これにより Darktrace は脅威の最もかすかな兆候に対してもリアルタイムで自律的に検知および対処することが可能となり、被害が発生する前に悪意あるアクティビティを封じ込めることができます。

Darktrace Antigena は、高度に標的型でまったく未知のものであっても、動きの速いランサムウェアをマシンスピードかつ正確に的を絞って遮断できる唯一のテクノロジーです。24 時間の防御を提供する Darktrace は、チームが業務に圧倒されている、準備ができていない、あるいは単に人がいない場合にも、深夜、週末、休日に関係なく、重要なデータおよびシステムの安全を守ります。

医療従事者の仕事を可能にするシステムおよびデータへの中断のないアクセスの確保は、最優先でなくてはなりません。Cyber AI を導入することで、悪意あるアクティビティに対する 24 時間、週 7 日にわたり自動対処技術が稼働することにより動きの速い脅威が出現次第その拡散を阻止することができるため、自己防御型のデジタルエコシステムが実現できます。

暗号化の前にランサムウェアを阻止

ランサムウェア攻撃に遭遇したとき、組織にとって最悪の事態はセキュリティチームが不在であることです。しかし、ある Darktrace の顧客においてまさにこうした事態が発生しました。

最初の侵害が発生したのは、1 人の従業員が会社用スマートフォンから個人用メールにアクセスし、騙されてランサムウェア週 7 日にわたり自動対処技術が稼働することにより悪意のあるファイルをダウンロードさせられたときでした。 数秒後には、彼の端末は Tor ネットワーク上の外部サーバーに接続し、SMB 暗号化アクティビティが開始されました。 わずか 9 秒以内に、Darktrace はこれを検知し優先度の高いアラートを生成し、この未知の動作に対して即座に調査が必要であることを知らせました。

この動作がその後数秒間継続すると、AI は脅威の深刻度に対する判定を更新しました。 この時セキュリティチームは既に帰宅し週末の休みに入っていましたが、幸いなことに Darktrace Antigena が設定されており防御の準備ができていました。Darktrace の AI が単独で攻撃を阻止し、暗号化されたファイルをネットワークファイル共有に書き込もうとするすべての動作を中断した結果、1 つのファイルも暗号化されずに済みました。

Darktrace Antigena を使っていなければ、セキュリティチームは月曜日出社したときにはカオスに遭遇していたでしょう。 Darktrace が提供する、組織の DNA に対する深く変化する理解によってのみ、洗練されたランサムウェア攻撃に対してもこのようなリアルタイムの検知および対応を行うことができます。

"AI が組織と患者情報を守ってくれているため、夜も安心して眠れるようになりました。"

Penn Highlands Healthcare 社、CIO、トム・ジョンソン氏

"Darktrace の自己学習能力は状況を一気に変える力を持っています。これまでに見たことのない潜在的な脅威を見つけ出す独自の力を備えているのです。"

Swope Health Services 社、CIO、ブライアン・トーマス氏

Darktrace Antigena が進行中のランサムウェアをピンポイントに的を絞って阻止