アイティフォー　CyCraft AIR（サイクラフト・エアー）

AI型EDRが侵入“後”の対応を高速・低コストに 数週間かかる「フォレンジック」が最短３時間！

侵入“後”の対応力強化が、被害最小化のカギを握る――。今やセキュリティ対策の常識だ。しかし人材不足に悩む企業にとっては、膨大なログを分析するなどの検知後の対応は容易ではない。そこで有効なのが“AI”である。アイティフォーが提供するCyCraft AIRは数週間かかる作業を最短３時間以内に完了できるなど、高速な対処を可能にする。

最近の企業は”国家レベルに高度化、巧妙化したサイバー攻撃”に狙われるようになっている。

2021年上半期、米石油パイプライン最大手のコロニアル・パイプライン社がサイバー攻撃を受けた事件は記憶に新しい。米国東海岸のジェット燃料やディーゼル、ガソリン燃料などの主要貯蔵庫がランサムウェアにより大きな影響を受け、一部の操業が５日間にわたり停止した。経営者は440万ドル（約４億8000万円）の身代金を支払ったとされる。米連邦捜査局（FBI）は一連の犯行をハッカー集団「ダークサイド」によるものだと結論付けた。

「こうしたサイバー攻撃集団は、非常に強力なツールを用いて巧妙に攻撃を仕掛けてくるため、ファイアウォールやアンチマルウェアなど、従来のセキュリティ対策だけでは被害を防げなくなっています」（アイティフォー 通信システム事業部 営業一部 部長 羽田誠氏）。

質だけでなく、量の面でもサイバー攻撃の脅威は増している。「コロナ対策に伴いリモートワークやシステムのオンライン化が進んだことで、フィッシング攻撃を含めたサイバー攻撃が増加しています」と羽田氏は警告する。

金融機関や自治体など、セキュリティ対策を重視している組織においても近年被害は拡大している。「これらの業種では、セキュリティ面が脆弱な古いOSでシステムを動かしているケースが少なくありません。そういったシステムは従来、社内ネットワーク内で稼働しインターネットから隔離されていましたが、最近ではAPIなどを介して外部と繋がることが多くなっています。そのため、狙われやすい状態になっているのです」と羽田氏は指摘する。こうした背景から、セキュリティ対策における“常識”もここ数年で変わってきた。

AIによる高い検知率 台湾発ベンダーの高性能EDR

「今までは防御策を高く積み上げて、水際で侵入を防げれば良いという考え方でした。しかし検知しきれない攻撃が増えてきていることから、守れないことを前提に考える必要があります」と羽田氏は解説する。

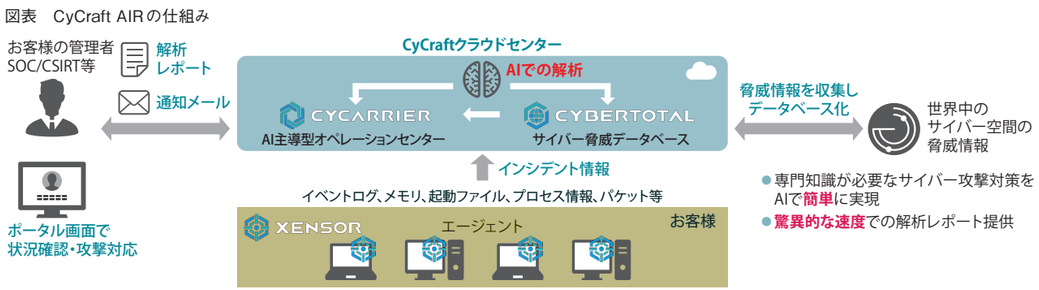
アイティフォー 通信システム事業部
営業一部 部長 羽田誠氏

被害を拡大させないように、感染端末を隔離したり、情報流出の有無を把握するための調査を迅速に行ったり、侵入後の対策が重要になっているのだ。

その具体策としてアイティフォーが新たに提供するソリューションが、AI主導型のサイバー攻撃対策サービス「CyCraft AIR（サイクラフト・エアー）」である。

CyCraft AIRはいわゆるEDRと呼ばれるもので、ユーザーが利用するPCやサーバーなどのエンドポイントにおける不審な挙動を検知し可視化することで、セキュリティチームが素早く対策をとることを可能にするソリューションだ。

図表　CyCraft AIRの仕組み



強みの1つが、検知率が高く誤検知も少ない、高品質なクラウドAI。米国の政府系非営利団体、MITRE社が2020年に21社の製品をテストしたところ、CyCraft AIRは検知能力と誤検知の分野で最高得点を獲得した。高い脅威の検知率を謳う製品は多いが、現場の負荷を考えると誤検知の少なさも同様に重視すべきだろう。

「同ソリューションを提供しているCyCraft社は台湾発祥のセキュリティベンダーです。台湾は中国系ハッカー集団から頻繁に攻撃を仕掛けられているといわれていますが、そうした危機意識の高い国の政府機関や金融機関において採用されています」と羽田氏は紹介する。

CyCraft社は政府機関などが参加するフォーラムなども含め、20を超える情報源から脅威インテリジェンスを構築し、脅威の検出に活用している。具体的には各エンドポイントからイベントログなどの情報を収集し、クラウドまたはオンプレミスのサーバーに展開したCyCraft社の脅威検知エンジンが分析。マルウェアおよび、マルウェアの被害に遭った感染端末などを検出する。

なお、クラウドは日本国内にも展開されており、データが国外に出ることもない。エージェントレスでの実装も可能で、柔軟に導入できる。

CyCraft AIRのAIエンジンが可視化した脅威状況。検出したアラートを分析し、ストーリーラインによって感染した端末やその感染経路などをダッシュボードにまとめてくれる。レポートは任意のタイミングで作成でき、緊急時でなくとも定期的に詳細な分析結果を提供する

フォレンジックを自動化 レポートも即提供

さらにCyCraft AIRの特徴としては、脅威の検知後、「フォレンジック」を自動で行ってくれることも挙げられる。フォレンジックとはデバイスやネットワーク内のデータをコピーし、そのコピーをもとに脅威の原因や状況などを解析するプロセスのことだ。重大なセキュリティインシデントが発生した時にフォレンジックは欠かせないが、高額な費用や人材・工数の確保が必要になる。

「サイバー攻撃の侵入を検知した後は、原因の究明や影響範囲の調査など行う必要があります。しかし、迅速な調査には豊富な専門人材が必要であり、外部へ依頼する場合のコストも一般的に高額です。大企業ほど組織やシステムが増えて調査の難易度が高くなるでしょう」と羽田氏は語る。

CyCraft AIRでは、このフォレンジックに必要な一連のフローをAIにより自動化することで、即座に感染状況と原因を分析し、的確な対応方法を提案する（**図表**）。本来はセキュリティ人材が必要な、各端末に分散している膨大なログやデータの調査・分析のための工数を大幅に削減できるのだ。誤検知の少なさと合わせて、セキュリティ人材不足に悩む企業にとって特に有用なソリューションである。

具体的には、脅威が検出されるとすぐにフォレンジック調査が自動で開始され、すべてのエンドポイントやプロセス、ファイル、ID、およびIDごとの権限情報などをスキャンする仕組みになっている。

スキャンした結果はクラウド上のAIが分析し、感染したエンドポイントや感染経路を可視化して、攻撃状況をわかりやすくレポートする。復旧作業にかかる時間を以前より短くできるだけでなく、対応方法もレポートとして提供するので、ユーザー企業が自社で対応できる。被害を軽減しつつ、企業の信頼回復に向けて迅速な対処を可能にするのだ。

驚くべきはその速度。CyCraft AIRは検出から最短で３時間以内に自動でレポートを提供することが可能だ。「人手でやると早くても2～3週間、場合によっては１カ月以上かかります」（羽田氏）。

IPA（情報処理推進機構）の「IT人材白書2020」によれば、セキュリティ人材を十分に確保できていると考えている組織は10％ほどに過ぎない。「そこで、我々の提供するCyCraft AIRによって限られた人材でも効率的に対処できるようにしていこうと提案しています」と羽田氏は語る。「当社のユーザーには地方の銀行や自治体も多くいますが、地方では専門人材の不足が大きな課題です。人材不足に喘ぐ企業にこそ有用なソリューションと考えています」

脅威を検知できるだけでなく、少ないリソースでその後の被害も最小限に抑えられるCyCraft AIR。あらゆる組織にとって、頼もしい武器になってくれるだろう。

お問い合わせ先
株式会社アイティフォー
通信システム事業部
TEL：03-5275-7909
E-mail：info@itfor.co.jp