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。

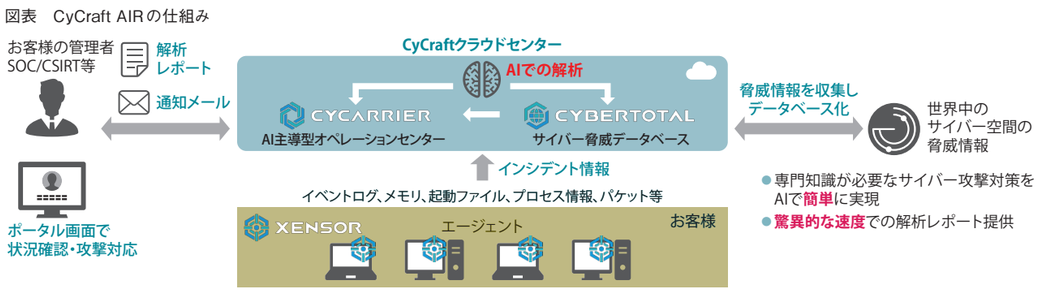
アイティフォー 通信システム事業部
営業一部 部長 羽田誠氏

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。

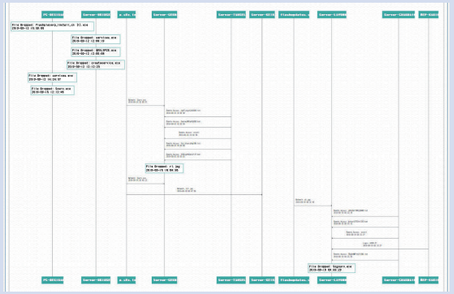
お問い合わせ先
株式会社アイティフォー
通信システム事業部
TEL：03-5275-7909
E-mail：info@itfor.co.jp

アイティフォー　**AI主導型EDR「CyCraft AIR」**

なぜ、AI主導型EDRなら短期解決？インシデント対応の４つのポイント

サイバー攻撃はもはや避けようのない「経営リスク」だ。そこで重要なのがいかに短期に終息させ、被害を最小限に食い止めるか――。セキュリティ専門家のいない“ごく普通の企業”でも、AI主導型EDR（Endpoint Detection and Response）があれば、悪意のある攻撃の発見から緊急対応、原因と被害の全容解明、報告書の作成までを高速に自動化可能だ。

CyCraft AIRの必要な情報に絞った分かりやすいレポート画面。より詳細な情報が必要な場合は、管理画面のドリルダウンで確認が可能



どのように感染が広がっていったのか、ストーリーライン（タイムライン）によって時系列で追うことも簡単

今年夏、あるセキュリティインシデントに大きな注目が集まった。東証一部上場の有名企業が、サイバー攻撃により決算発表の延期を余儀なくされたのだ。同社が、サーバーのウイルス感染によるシステム障害発生の第一報を出したのは7月初旬。その後、1カ月以上が経過しても、財務会計システムなど一部システムが利用できない状況を脱せず、8月中旬に決算発表の延期を公表した。

上場企業にとって決算発表の延期は、きわめて深刻な「事件」だが、残念ながら同社のようなケースは、もはや異例の事態とはいえない。影響が広範囲にわたり、被害も長期化するインシデントが頻発しているからだ。

「今回の事件のように、データの漏洩・破壊の発覚後、被害の全容把握や対処の完了まで時間がかかるケースは非常に多いです。迅速に対応するために必要な体制が揃っていない企業が大半だからです」と総合ITベンダー、アイティフォーの羽田誠氏は解説する。

サイバー攻撃の完全なブロックが不可能ということは今や「常識」だ。インシデントは必ず発生する。つまり、いかにインシデントを短時間で終息させ、被害を最小限に抑えるかが重要なわけだが、この「インシデントを迅速に終息させる」ための体制が多くの企業に欠けているというのである。

とはいえ、ごく一般的な企業が、セキュリティツールや人材などに多額の投資を行なうことは難しい。一体どうすればいいのだろうか。

羽田氏は4つの問題解決ポイントに整理して具体策を伝授する。解決の扉を開くのに必要なのは、たった1つのセキュリティツールだ。詳しく見ていこう。

インシデントが起こると実際どんな対応が必要なのか？

羽田氏が推奨するツールは、今や世界有数のIT先進国として知られる台湾のAIセキュリティベンダー、CyCraft社のAI主導型EDR製品「CyCraft AIR」である。「専門家や多くの人手に頼る必要があった分析作業を、AIが短時間で詳細に行ってくれます」と紹介する。

では、実際にインシデントに遭遇したとき、CyCraft AIRはどう活躍するのか。それを見ていく前に、インシデント対応の一連の流れを追ってみよう。

セキュリティツールによる検知、社外からの連絡……。発覚の仕方は様々だ

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

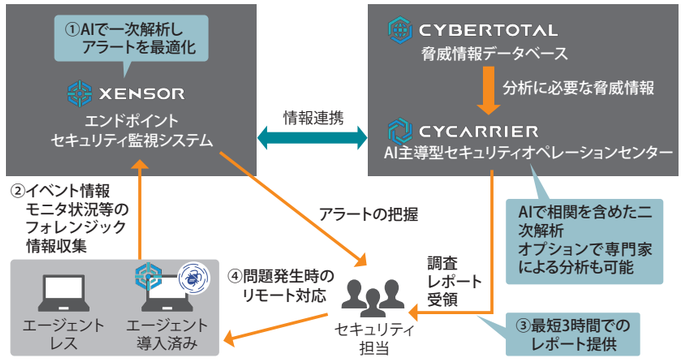
が、どのような形にせよインシデントが発覚するとまず必要になるのが「初動対応」だ。「一般の事件・事故と同じように、被害を拡大させないためには、初動対応が非常に大切になります」と羽田氏は指摘する。

初動での緊急対応が一段落したら、インシデントの終息に向けて、「調査方法等の計画立案」と「証拠保全」を行いながら、原因や被害の全容解明や復旧作業などの「調査・対処」を実施。

そして、最後に原因や被害の全貌を「報告・公開」して、インシデントは終息を迎える。報告書の公開などにより、インシデントを明確に終息させないと、漫然とした調査や目的不明な対応が延々と続くことになりかねない。

以上がインシデント対応のおおまかな流れだが、CyCraft AIRはそれぞれのフェーズで効果的な対処を行うためのAI機能を揃えている。社内にセキュリティの専門家などいない普通の企業が、短時間でインシデントを終息させ、被害を最小限に食い止めるためのAI機能だ。

図表　CyCraft AIRの構成



AIで発見・解析を高速自動化 未導入端末まで網羅的に調査

4つの問題解決ポイントに分けて、CyCraft AIRの特徴を説明しよう。1つ目のポイントは「早期発見」だ。

CyCraft AIRは、エージェントレスモードでは日次ペース、エージェントモードでは常時、エンドポイントを監視して悪意ある挙動を検知する。どの端末が被害に遭い、被害の範囲はどこまで広がっているかを短時間で可視化することが可能だ。

注目すべきは、その誤検知率の低さだ。米MITRE社が2020年に行った「MITRE ATT&CK評価テスト」の検知分野で、21社の製品中、最高のスコアを獲得した。

「他社のEDR製品の場合、あまりに多くのアラートが上がるため、管理者がパンクして重要なアラートを見過ごしがちです。これに対してCyCraft AIRは、本当に対処が必要なものに絞り込むため、運用負荷が非常に少なく、かつ必要な対応をしっかり行えます」

早期発見のみならず、早期対応を実現できるのである。

「最近のマルウェアは感染力が強く、1台に感染すると、次々に他のサーバーなどへ感染を拡大していきます」と羽田氏は言う。冒頭に紹介したインシデントも、あと少し早期発見できていれば、財務会計システムまで被害が及ばなかったかもしれない。

2つ目のポイントは「網羅性の向上」だ。被害状況の一部しか分からないようでは、インシデントの全容など掴みようがない。CyCraft AIRの場合、事前に導入していなかった端末でも、フォレンジックベースで網羅的に解析できる。

「通常のアンチウイルスやEDRは、その製品が入っていないと調査できません。また、感染端末は現場で工場出荷時の状態に戻してしまい、ログが残っていないというケースもよく聞きます。私用端末の業務利用も含め、過去に何が起こったのか、網羅的に証拠保全・解析できる仕組みが必要です」

3つ目は「調査の高速化」だ。感染端末の隔離やサービス停止などの応急処置は済み、調査に必要な証拠も集めた。しかし、これで終わらないのがインシデントのつらいところだ。収集した膨大な証拠を人手で分析し、原因や被害の全容を解明するには、高い専門性と多くの労力が必要になる。しかも、調査に手間取り、最終報告が遅れるほど、企業の信頼はいっそう低下していく。

だがCyCraft AIRなら、様々なセキュリティ組織などから収集した脅威インテリジェンスも活用しながら、AIがログデータなどを自動で相関分析してくれる。「人手なし、最短3時間という迅速さで詳細に分析できる製品は、なかなか他にないはずです」

報告書の作成・出力も自動で可能だ。「他社のEDRにも自動レポート機能はありますが、専門家以外には分かりにくいレポートです。一方、CyCraft AIRの自動レポートはほどよい詳細さ。専門家でなくても理解できます。さらにオプションで、CyCraft社のセキュリティエキスパートによる調査・分析をプラスできます」

最後の4つ目は「リモート調査・対応」だ。テレワークが広まった今、遠隔からも原因調査や感染端末の隔離などができなければ、迅速な対応は到底実現できない。CyCraft AIRは、調査や隔離対応もリモートで実施できる。

このように、インシデントの早期発見から報告書の作成・公開による終息までを、1つのツールで高速に進めることが可能なCyCraft AIR。セキュリティが重大な経営リスクになった現代、企業の強力な味方になるだろう。

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