VECTRA
SECURITY THAT THINKS

Eブック

サイバーセキュリティのギャップを埋める新たな脅威検知モデル

DATA SCIENCE
OPERATIONAL EFFICIENCY
CLOUD-NATIVE
ENTERPRISE

見過ごされているサイバーセキュリティのギャップ

境界線セキュリティの防御システムをすり抜けて標的組織に侵入した攻撃者が、最終的な重要資産の窃取や破壊に至るまでの間には、サイバーセキュリティのギャップ（死角）が存在します。

このギャップでは攻撃者のほうが、防御ベースの従来型セキュリティ製品に比べて圧倒的に有利です。防御ツールや手法は広く浸透していますが、サイバー犯罪者は常に、防御ツールを出し抜くための複雑で巧妙な攻撃方法を仕掛けてきます。

サイバー攻撃はもはや、事前にプログラミングされたマルウェアを使った単純なsmash-and-grab（強引な突破・窃取）手法ではなく、高度なスキルと創造性を備えた知的な人間がコントロールする攻撃に変貌しています。人間同士の継続的な連携により、標的ネットワークの情報を蓄積し、個々の防御対策に合わせて手法を変え、攻撃を徐々に進化させることができるのです。

攻撃手法は飛躍的に進歩して巧妙化しましたが、セキュリティ防御対策はこれに追いついていません。セキュリティ担当者は、既知の脅威やマルウェアの高速パターンマッチ（シグネチャ方式）による脅威検知作業で手一杯です。

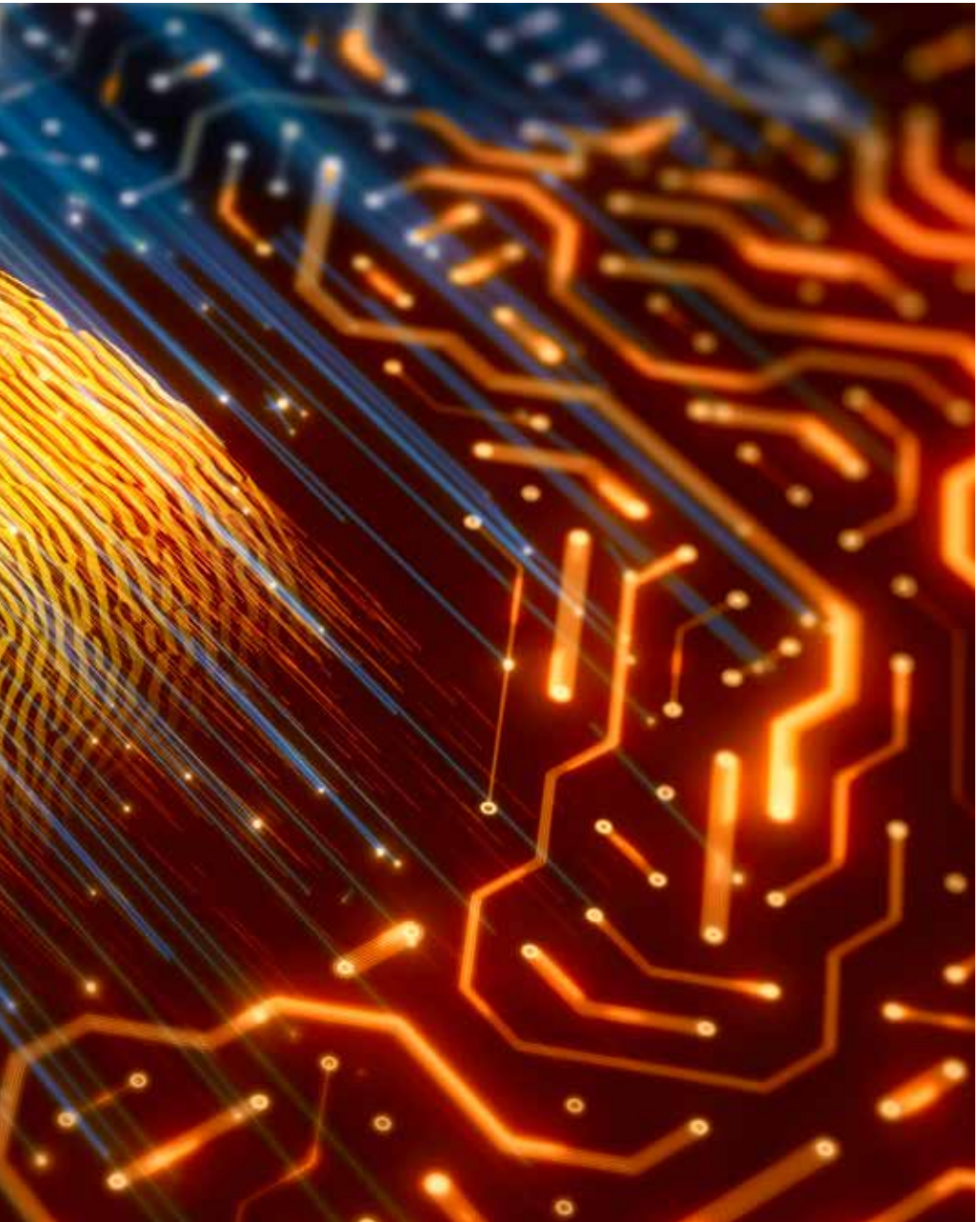
脅威の形態が徐々に高度化・巧妙化する一方、従来型のセキュリティ対策は「不完全な情報にもとづく瞬時の判断」から脱却しきれていません。

従来型のセキュリティは依然として「不完全な情報にもとづく瞬時の判断」に頼っています。

この不均衡な状況では、攻撃者が圧倒的に有利です。攻撃者に後れを取らないためには、よりインテリジェントなセキュリティ対策、すなわち「学習し、進化し、自ら思考する新たな形のセキュリティ」が必要です。

70-90%

マルウェアサンプルの70〜90%は、標的組織の特性に合わせて作成されたものでした。



本書では、過去の学習データおよびローカルコンテキストをもとに脅威を検知し、事象を時系列で相関付けることによって現在進行形の攻撃をあぶり出すための新たな方法論、およびその実践に必要な条件について解説します。

シグネチャ方式の課題

これまでの防御対策では、攻撃者に後れを取らないためにシグネチャの種類を次々に増やし、配信サイクルを短縮化してきました。従来型セキュリティテクノロジーの基盤であるシグネチャの目的は、悪意ある攻撃、悪性のURLおよび既知のマルウェアを特定することです。

シグネチャを使うと、既知の脅威を迅速に特定して一括ブロックできます。しかし弱点は、単純化方式であることです。アプリケーショントラフィックに遅延をきたさないようにマイクロ秒単位でYes/Noを判断するには、既知の脅威を最も単純なフィンガープリントに落とし込む必要があります。

単純に良性、悪性を瞬時に導き出す従来型の防御手法に対して、適応力のある攻撃者は優位に立つことができます。シグネチャは、既知の脅威に対するフィンガープリントとの照合で初めて機能しますが、新たな未知の脅威を用いてシグネチャを迂回する術を、攻撃者側は身に付けたのです。

この傾向が如実に表れているのが、ベライゾン社の2015年度データ漏洩・侵害調査報告書です。報告書には「データ侵害に使われたマルウェアの70～90%が、当該マルウェアに感染した組織に合わせた特性をもっていた」とあります。

つまり防御対策としては、スケールメリットのない「自組織固有のシグネチャ」を使う必要があります。しかし、未知の脅威やゼロデイ脅威が悪用された場合、それらを検知できるシグネチャは存在しないため、攻撃者にとって「シグネチャの迂回」が簡単かつ重要な攻撃手段であることに変わりません。

攻撃者はシグネチャの先手を打つことができますが、攻撃者優位となった真の理由は、攻撃スパンの持続性にあります。対外的な防御線さえ侵害すれば、標的組織のネットワーク内に紛れ込み、偵察を重ね、深部の層にまで攻撃を拡散して、窃取または破壊に値する重要資産を見つけ出すことができてしまうのです。

このプロセスを進めるには通常、侵害されたホスト（複数）、各種ツールとマルウェア、窃取して不正利用するための正規ユーザーの認証情報が必要です。重要な点は、攻撃者が時間をかけて作戦の進化や適応を重ねている間も、脅威自体は進行中であるということです。

攻撃者が時間をかけて作戦の進化や適応を重ねている間にも、脅威自体は進行しています。

シグネチャ方式の検知システムは、脅威を極小レベルまで単純化して特定するため、その周辺で起きている複雑な化学反応（各要素の相関性）を認識するには大変不向きです。こうして生じたインテリジェンスのギャップを埋めるためにも、脅威検知における新たなセキュリティモデルが不可欠です。

脅威検知における新たなモデル

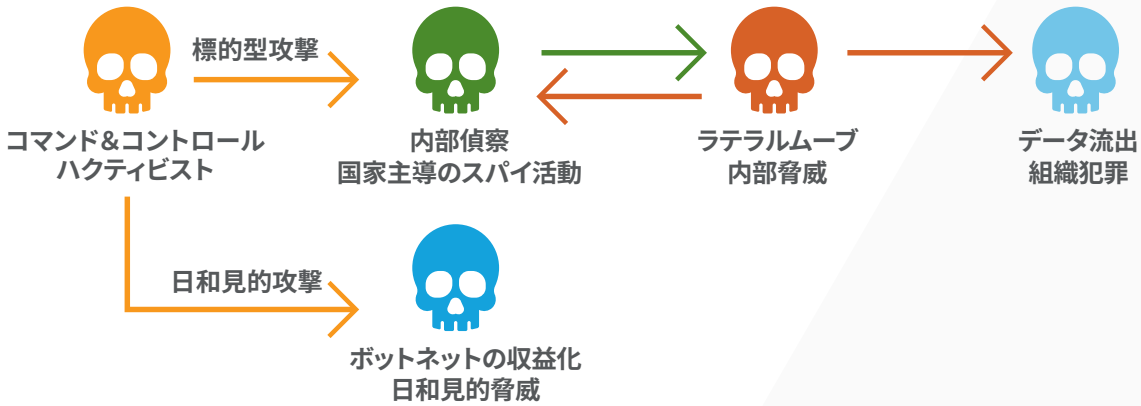
最新かつ最先端の脅威検知モデルは、従来型セキュリティテクノロジーが検知できないギャップを埋められるだけではありません。長きにわたって戦略的優位性を享受してきた攻撃者を抑え込む効果もあります。

粗い粒度で効果が限定的な検知情報

攻撃者がシグネチャによる検知を迂回するために新たなドメインに移動したり、既知のマルウェアを加工（ビット数を多少追加）して適応するたびに、シグネチャベースの従来型検知システムは陳腐化していきます。これにより、攻撃者はマルウェアを小手先で加工するだけでも防御側の数歩先の立場を維持でき、先行者としてのメリットを得られているのです。

新たな脅威検知モデルの大きな目的は、長期間にわたり 有効な検知結果を提供することです。そのためには、脅威の対象となる個別インスタンスすべてのフィンガープリントを取得するという手法から脱却し、「すべての脅威に共通する根本的な攻撃特性の把握」に焦点を移す必要があります。

パケットレベルのトラフィックにデータサイエンスや機械学習などのツールを適用すると、通常のトラフィックとは異なる「脅威の本質」を効果的に顕在化できます。



攻撃者の行動と振る舞いを重視する

従来型の検知モデルでは、悪用攻撃に使われるコードのスニペット、既知のマルウェアサンプルまたは悪質ドメインの特定を試みます。つまり、次々に発生する悪質な事象をすべて特定し、フィンガープリントを登録する作業が無限に繰り返されます。こうした状況では、新たな悪用手段を用いる攻撃者は常に防御側の数歩先にいます。

新たな脅威検知モデルでは、この悪循環を断ち切るために、ありとあらゆる悪質な事象をすべて羅列する代わりに、「攻撃者の振る舞いや行動特有の痕跡」を特定することに軸足を移します。

つまり事象そのものではなく、事象によって何が起こるのかを解明することが目的となります。マルウェアを微調整したり新たなドメインを購入して脅威検知をすり抜けることはできても、攻撃者の行動やその目的は常に変わらないからです。

たとえば、攻撃手法の連携や管理のやり取りをするために、ほぼすべての攻撃で何らかの隠れた通信チャネルが必要になります。さらに、標的環境の内部で拡散してデバイスや認証情報を次々に侵害し、最終的に標的組織の資産を破壊する、またはネットワーク外に持ち出すという工程も必要です。

攻撃手法の連携や管理のやり取りをするために、ほぼすべての攻撃で何らかの隠れた通信チャネルが必要です。

攻撃の振る舞いを重視することで、防御側に有利なセキュリティの基軸を回復し、圧倒的に劣勢なサイバーセキュリティの戦いを勝ち抜くことができます。何千個ものシグネチャを使って脅威の亜種すべてを特定する代わりに、攻撃を完遂するために必要な振る舞い（主なものは数十種類）の見定めに焦点を絞ることができます。

脅威の経時的変化を理解する

今日のネットワークデータ侵害において最も顕著な特性のひとつは、脅威が徐々に進化するという点です。高度な攻撃では、このように少しずつ目立たずに実行する(low-and-slow) アプローチが標準手法となっていますが、これには正当な理由があります。従来型のセキュリティ対策には、記憶が短期間で消滅すること、および侵害後の履歴を一切記録できないという弱点があるためです。

従来型セキュリティ対策の弱点は、記憶が短期間で消滅すること、および侵害後の履歴を一切記録できないことです。

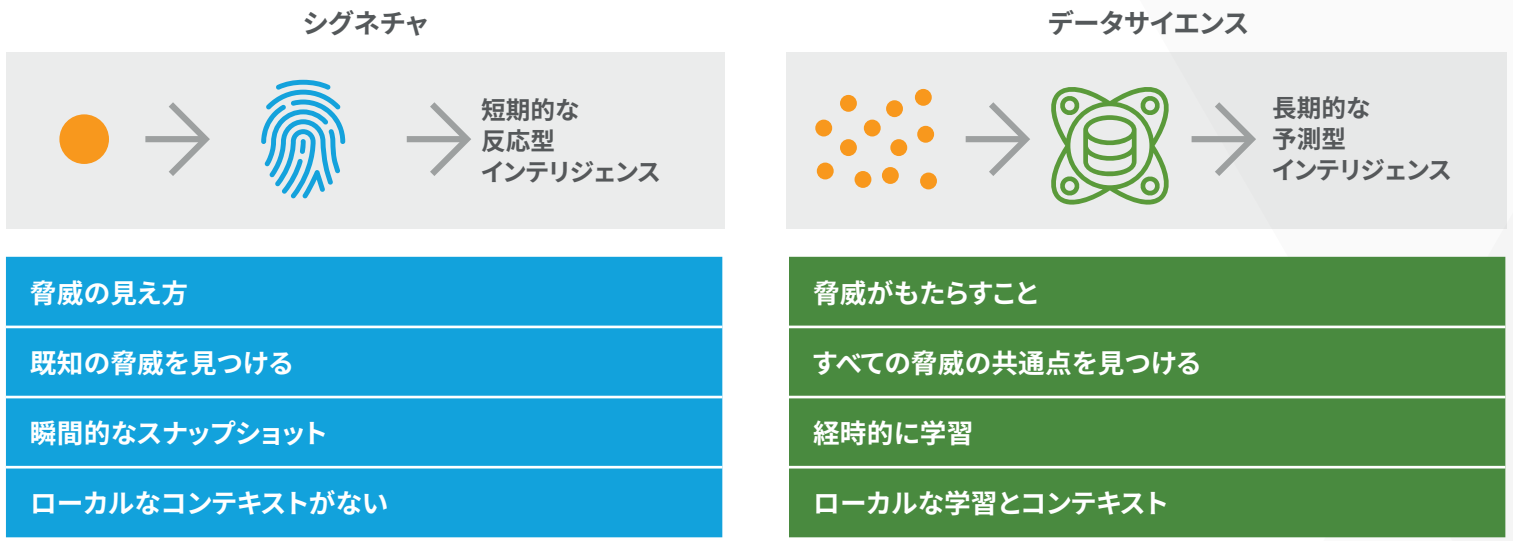
新たな脅威検知モデルでは、脅威をリアルタイムで認識しつつ、徐々に進化する攻撃の兆候も特定します。どちらかが犠牲になることはありません。たとえば、ネットワークセッションの発生タイミングや間隔のわずかな乱れによって、攻撃用の隠れたトンネルやリモートアクセスツールをあぶり出すことができます。

反対に、「従業員の認証情報が侵害された」という事象を認識するためには、数日、数週間または数ヵ月かけてユーザーの通常時の振る舞いを学習しなければならないかもしれません。学習期間がごく短期間であっても長期に及ぶ場合でも、対象期間における脅威の内容を徹底的に理解する必要があります。

手法だけでなく、攻撃そのものを理解する

セキュリティ対策の価値は、大量のアラートをただ配信することではなく、組織にとっての真のビジネスリスクを特定することです。そのためには、個々のイベントの相関性および、これらの脅威が組織の資産に与える影響を、セキュリティソリューションで認識できるようにする必要があります。

こうした機能を実現するには、脅威のコンテキストと組織固有のコンテキストの両方が必要です。攻撃の各段階に発生する点と点を結んで全体像を明らかにできれば、ネットワーク上で日々大量に発生するコモディティ型の脅威と標的型攻撃を区別できます。



データサイエンスを使った脅威検知

データサイエンスと機械学習の手法をネットワークトラフィックに直接適用すれば、前述の機能を実現できます。最新の脅威検知モデルでは、ネットワーク内部に潜む攻撃者をすばやく検知するために、データサイエンスと機械学習の両方を採用しています。

データサイエンスの活用目的

「データサイエンス」や「機械学習」という言葉がセキュリティ業界を席巻し、その効果や用途が次々に出てきました。しかし、これらはあくまでもツールであり、セキュリティの問題をすべて解決する万能策ではありません。

宣伝文句に踊らされないためには、データサイエンスや機械学習を用いたアプローチがどのような価値をもたらすのか、他のアプローチとどう異なるのか、さらにはメリット・デメリットに至るまでを正確に理解する必要があります。

データサイエンスはセキュリティのありかたを抜本的に変えます。脅威と対応策を1対1で照合するシグネチャベースの方式と違い、データサイエンスでは過去に観測された脅威すべての集合知をもとに、新たに出現した脅威をすばやく特定します。

新しい科目を勉強する学生をイメージしてください。解答を丸暗記すればテストで合格点を取れるかもしれませんが、「問題の解き方」を理解してはいません。

長期的には「何を、いつ、なぜ、どのように」の部分を理解することが不可欠です。これまで見たことのない新たな問題を評価し、解決するためには、実際の知識とインテリジェンスを身に付けておくほうが圧倒的に有利です。

この点こそ、従来型モデルとデータサイエンスを用いた脅威検知のアプローチとの大きな違いです。従来型モデルは、すべての解答をあらかじめ知っておくこと（既知であること）が条件です。たとえば「ACME.comというドメインで悪意ある振る舞いが過去に確認されている、したがって当該ドメインは悪質である」という考え方です。

データサイエンスでは、現実の質問に集合知を適用して未知の対象物を評価します。

たとえば「これまでACME123.comによる悪意ある振る舞いは確認されていないが、当該ドメインを出入りするトラフィックで4パターンの振る舞いが確認されている。これらを組み合わせると、コマンド&コントロール攻撃の振る舞いと一致する」などのシナリオがあります。

脅威に関する実世界の集合知を反映した結果、「このような振る舞いをするドメインは悪意がある」と判断できるのです。

生のデータに直接触れることの重要性

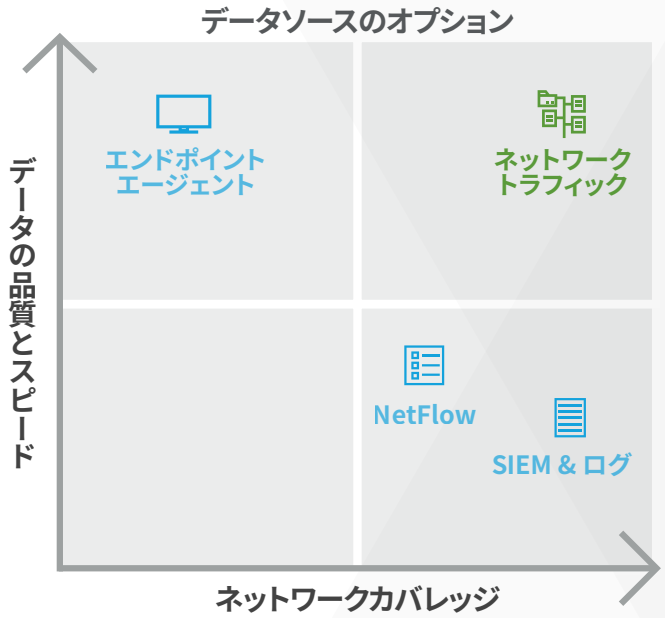
データサイエンスのモデルは本質的に分析対象データの質に依存し、とくにサイバーセキュリティ領域ではそれが顕著です。サイバーセキュリティ対策ソリューションの重要な役割は、従来型セキュリティのコントロール機能をすり抜ける、ステルス性の高い脅威を特定することです。そのためには、ネットワークトラフィックすべてに直接アクセスし、実際に確認する必要があります。

一般的にデータサイエンスを使った脅威検知では、イベントログの大規模データベースに対するデータマイニングを実行します。このアプローチでは、これまで見過ごされていたログ同士の相関関係を特定できる可能性もある一方、課題もあります。

ログは、事象を簡潔にまとめた副次的データです。ログにない情報は消失し、分析することができません。さらに、ログを生成するシステムの精度にも左右されます。上流工程のファイアウォールやセキュリティデバイスで脅威を検知できなければ、分析するためのログも残りません。

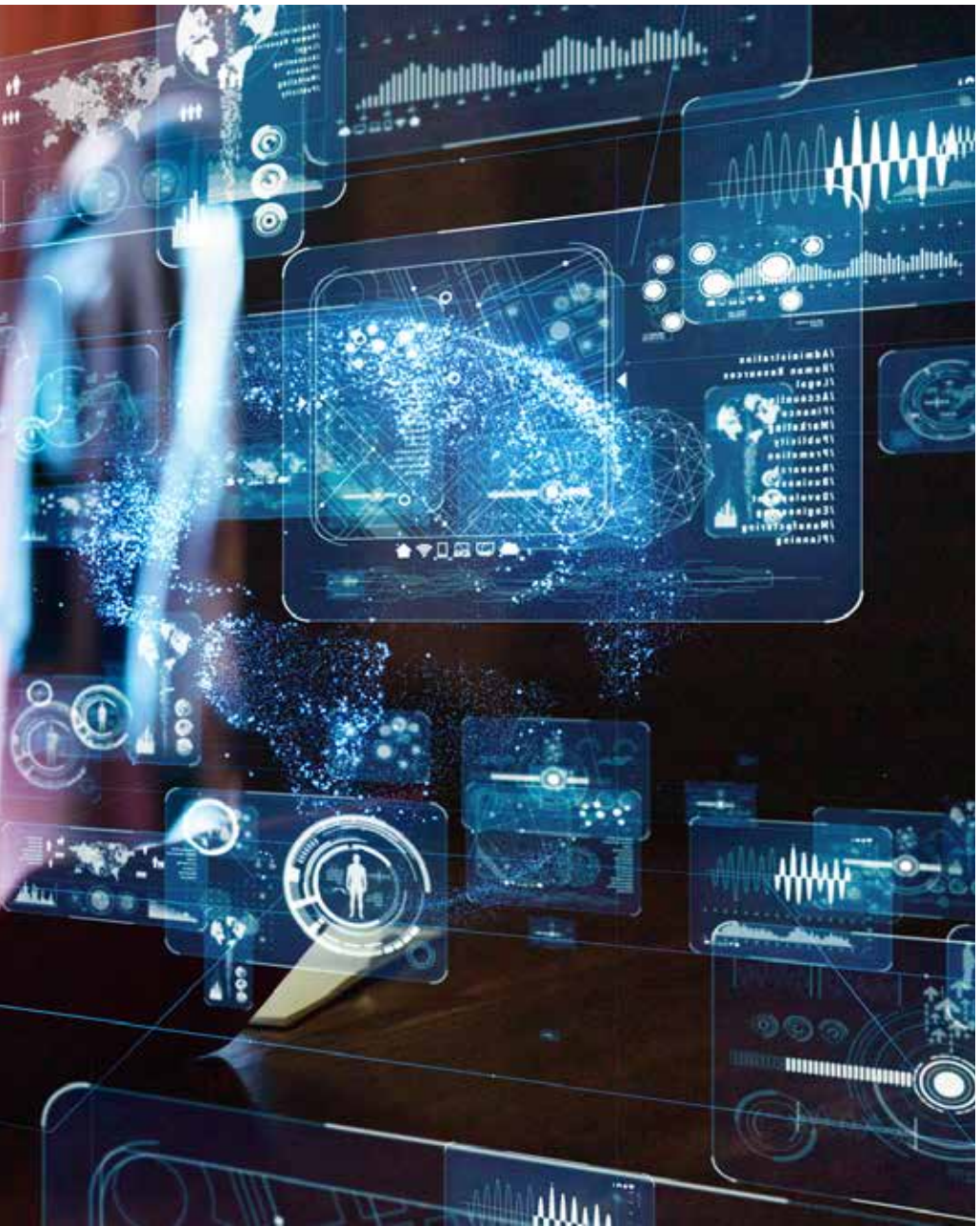
ログデータの限界は不安材料となります。サイバーセキュリティソリューションの役割は、通常の防御層をすり抜ける脅威を検知することです。脅威を検知できなかったデバイスから提供されるサマリー情報を再分析することは、理にかなっているとは言えないでしょう。

脅威を検知できなかったデバイスのログを再分析することは、理にかなっているとは言えません。



NetFlowをはじめとするフローサマリーの分析ツールも同様の壁に直面しています。フローデータは、ネットワークを流れるトラフィックのパフォーマンスを監視・追跡するものです。しかしこれらのツールが追跡するサマリー情報はネットワークトラフィックの方向やデータ量だけであり、検知の網を巧妙にすり抜ける隠れた脅威をあぶり出すために必要な、直接的なアクセスや可視性が得られません。

データサイエンスを使ったモデルは、適用するデータの質が高いほど大きな効果を発揮します。そこで新たな脅威検知モデルでは、不完全なソースが生成するデータを単純にマイニングする代わりに、ネットワークトラフィックのパケットレベルでデータサイエンスと機械学習を適用します。



このようにトラフィックそのものに直接アクセスすることで、まったく新たな形で脅威を検知できます。高度な脅威検知モデルでは、事象の関連付けや単純なベースラインの見極めではなく、悪意あるトラフィックの振る舞いをリアルタイムで認識します。

サイバー攻撃は常に進化します。しかし新たな脅威検知モデルは、トラフィックを常に直接可視化することで適応を繰り返し、新種の攻撃手法や戦略を特定できます。これは、上流工程のデータソースに依存せざるを得ないログベースやフローベースのシステムとは対照的です。

データサイエンスにおける機械学習の役割

人気と関心が高まるにつれ、「データサイエンス」と「機械学習」という言葉が便利なキャッチフレーズとなり、両者の違いがわかりづらくなっています。

データサイエンスとは、データからナレッジを抽出する方法全般を指します。数学、統計学、機械学習のほか、多種多様な分析学をはじめとする幅広い領域を俯瞰的にカバーします。

重要な点は、機械学習はデータサイエンスのサブセットであることです。教師あり・教師なしの機械学習、数理的なヒューリスティック検知モデル、統計モデル、振る舞い分析などを含む多種多様なデータサイエンス手法は、新たな検知モデルにも活用されています。

機械学習を使うと、データをもとにソフトウェアに反復学習させ、明示的にプログラミングしなくても適応させることができます。機械学習を脅威検知に適用すると、攻撃の特定につながる振る舞いパターンの識別、学習が可能になります。

機械学習を脅威検知に適用すると、攻撃の特定につながる振る舞いパターンの識別、学習が可能になります。

教師あり・教師なしの機械学習

脅威を検知するには、上位階層のデータセットが2種類必要になります。一つ目は、通常トラフィックや無害なトラフィックと脅威とを識別する、グローバルエクスペリエンスデータです。二つ目は、特定の環境における不審な、または異常な振る舞いを明らかにするためのローカルエクスペリエンスデータです。

一つ目は発生元ネットワークを問わず「常に悪質な」振る舞いを、二つ目はローカルコンテキストをもとに脅威を明らかにするためのアプローチです。いずれも脅威検知には不可欠であり、連動させる必要があります。

教師ありの機械学習は一つ目（グローバルデータ）を対象に、既知のマルウェア、脅威、攻撃手法を分析します。その後、すべての亜種に共通する「基本的な侵入後の振る舞い」をセキュリティリサーチャーやデータサイエンティストが特定します。この分析結果がアルゴリズムに反映され、ネットワークトラフィックの根底に潜む悪質な振る舞いを検知します。

グローバルインテリジェンスはきわめて有用ですが、なかには標的ネットワークのローカルコンテキストを把握しなければ検知できない攻撃もあります。教師なしの機械学習とは、特定のネットワークにおける通常の振る舞いと、基準を逸脱した振る舞いに対して先を見越して認識するモデルです。

教師あり、教師なしのスタイルはいずれも機械学習にとって不可欠であり、両者の連動によって隠れた脅威を検知します。同様に、長期間にわたって両者が観測したデータが検知アルゴリズムの材料として活用されます。

新たな脅威検知モデルは、単一のパケットやデータフローをもとに数ミリ秒以内で結果を導き出す代わりに、一定の期間（数秒から数週間）にわたって攻撃の振る舞いパターンを学習し、攻撃を特定します。

結論

最新かつ最先端の脅威検知モデルは、業界トップクラスの様々なインテリジェンスと検知手法を組み合わせ、あらゆる角度からリアルタイムで脅威を可視化します。従来のセキュリティモデルでは検知できなかった脅威をデータサイエンスで明らかにする、より効果的かつ斬新で高度な方法論です。

お問い合わせ：info-japan@vectra.ai　vectra.ai/jp