ThreatML：適切な機械学習

F5 の深層検出アプローチは、予測を活用することで、
調整の必要なく、実際の実行可能な脅威を表面化させます。

Google で「教師あり学習」と検索すると、これが機械学習（ML）と人工知能（AI）のサブカテゴリであることがわかります。

このモデルでは、ラベル付けされたデータセットを使用して結果を予測するためのアルゴリズムを学習しています。

クラウドセキュリティの世界では、これを予測型脅威モデリングと呼んでいます。
本 E ブックでは以下のことについてご説明いたします。

1. ThreatML™ + ルールがクラウドセキュリティに適した ML である理由

2. F5® Distributed Cloud App Infrastructure Protection（AIP）（以前の Threat Stack）の細部のテレメトリー収集とルールにより、有効性の高い脅威検出のための教師あり学習技術を開発することができた理由

3. クラウドセキュリティの未来が教師あり学習である理由

クラウドインフラストラクチャの最新化

組織は、コストを削減し、生産性と柔軟性を高めるために、アプリケーションとアーキテクチャの最新化をこれまで以上に重要視しています。実際、451 Research の最新調査によると、87% の組織が最新と従来の両方のアーキテクチャを運用していて、最新化は、柔軟性に欠けるレガシーシステムが急速に変化するビジネス環境に対応できないときに必要になると考えられています。[1] しかし、製品やサービスの急速な変化とデジタル化に取り組む組織は、特にサイバーセキュリティに関して新しい課題に直面しています。

現在行われているイノベーションのほとんどは、クラウド上で行われています。IDC Futurescape の最新レポートでは、世界中の推定 90% 以上の企業が、インフラストラクチャのニーズを満たすために、オンプレミス / 専用プライベートクラウド、複数のパブリッククラウド、およびレガシープラットフォームを組み合わせて利用しています。[2] そのため、セキュリティチームは、ワークロードの実行場所に関係なく、インフラストラクチャおよびアプリケーションのスタック全体において、セキュリティとコンプライアンスのリスクを効率的に特定し、対応する必要があります。

異種混在のクラウドインフラストラクチャ環境において、これは、クラウドネイティブの先進組織であっても、言うほど簡単なことではありません。

クラウドインフラストラクチャ全体のセキュリティにおける課題の評価

ほとんどの組織は、制約の中で可能な限り最善のセキュリティ運用を行うことを重視しています。制約とは、人手が足りない、予算が少ない、またはセキュリティ以外にも業務があることなどです。最善の運用とは、対象範囲、コンテキストおよびコストの適切なバランスを保つことです。セキュリティチームに求められることは、環境内のすべての脅威の可視化、組織のより重要なニーズに関連する適切なコンテキスト、そして最も重要なことですが、平均認知時間（MTTK）と平均応答時間（MTTR）などの主要なセキュリティメトリクスを短縮することです。

しかし、ご存知のように、アラートの数が多すぎると対応し切れず、攻撃者の行動が不明瞭になります。チームは、最も優先順位の高い脅威に焦点を当てなければ意味がありません。他のベンダーは、単なる異常検出でこの問題を解決しようとしていますが、コンテキストがほとんどなくベースラインから逸脱した異常を見つけるだけでは解決になりません。さらに、アラートを抑制することでアラート疲れを緩和しても、誤った安心感を与えるだけで、リスクを軽減または管理する戦略にはなりません。そのため、コンテキストに応じた優先順位の高いアラートによって、環境を完全に可視化することが不可欠になります。

「セキュリティ運用チームは、アラートが鳴りやまない環境を劇的に改善すると主張するプラットフォームに興味津々です。これは、車で言えば、車を整備工場に持っていき、ダッシュボードの点灯しているエンジン警告灯を消してもらうだけで、検査に合格できることと同じです。両者の良い点を取る、つまり、車に関して最も差し迫った問題をより深く理解する方法があります。これと同じ論理をクラウドセキュリティに適用できます。」

クリス・フォード（Chris Ford）
F5 プロダクト&エンジニアリング RVP

フルスタックの可観測性と適切な機械学習で、既知の脅威と未知の脅威を克服

今日のデジタル時代において、セキュリティ組織は、ビジネストランスフォーメーションの推進を支援する必要があります。しかし、テクノロジーの実現と、増え続けるセキュリティおよびコンプライアンス要件への対応を両立させることは、困難な戦いのように感じられます。

ThreatML は、ますます複雑化する IT 環境を考慮し、F5 の豊富なセキュリティテレメトリーとアラートルールの価値を取り入れて、この課題への対処を支援します。

F5 のルール +ML のアプローチにより、セキュリティチームは、MTTK と MTTR を改善して、調査と修復の工程を最適化できます。その結果、セキュリティチームは、組織がコンテナや Kubernetes などの戦略的かつ変革的なテクノロジーを採用しながら、適切なセキュリティおよびコンプライアンス対策を講じ、重要なシステムや機密情報を保護できるように強化できます。

その目的は、環境に対する実際の実行可能な脅威を示す有効性の高いアラートを提供する ThreatML を通じて、予測型の機械学習を活用できるようにすることです。

Distributed Cloud AIP の継続的な革新

ThreatML は、クラウドセキュリティにおける最新の問題に対応した業界初で唯一のソリューションです。検出の深度と幅を犠牲にすることなく、実用的で関連性のある発見を提供、つまり、完全な可観測性を犠牲にすることなく、最も優先順位の高いアラートのみを表面化させることができます。また、自動化されているので、調整やメンテナンスの必要はほとんどありません。

F5 の重要な差別化要因の 1 つとして、F5 のプラットフォームは、毎日 600 億以上のイベントを分析し、ルールと機械学習の両方を適用して、既知の脅威と未知の脅威を発見しています。F5 の新しい予測型モデリングでは、教師あり学習を使用して、組織に関連すること、つまり予測不可能な行動に基づいて、発見の優先順位を自動的に付けることができます。これにより、最終的には、社内セキュリティチームが行うべき調査量が減ります。

教師あり学習は、検出の範囲や適時性にギャップを生じさせることなく、すでにリソースが不足しているセキュリティチームの負担を大幅に軽減することを目的としています。

リスク予測のための、教師あり学習による ThreatML のビジョンについて

F5 の教師あり学習のアプローチは、ThreatML における次の自然な流れであり、セキュリティ運用と非常に強く関連するコンテキストにより、完全なカバレッジを提供します。教師あり学習の課題は、モデルをトレーニングするために大量のラベル付きデータが必要なことですが、F5 にはすでにリアルタイムのルールエンジンがあるので、ThreatML は、他のベンダーと比較して優れたインサイトを提供し、非常に効率的なデータのラベル付けを簡単にできます。

これらの機能により、F5 は、教師あり学習のパイオニアとして、有効性の高い脅威検出を業界に提供できます。ThreatML を強化することで、F5 の深層検出アプローチは、行動を起こすために必要なコンテキストを備え、迅速な修正を必要とするアラートを表面化させます。

教師あり学習では、脅威とならない行動をフィルタで除外できるという利点が追加されます。このような行動は予測可能なので、アナリストがこれらに直接注意する必要はなく、検出が完全であることを確信しながら、より少ないが優先順位の高いアラートに集中できます。

このような機械学習の進化における次のステップにより、Distributed Cloud AIP は、深い可観測性を犠牲にすることなく、既知の脅威と未知の脅威の両方について業界で最も関連性の高いセキュリティアラートを提供します。

仕組み：

ルールは、組み込み型であり、設定も可能です。つまり、既知のセキュリティリスクとコンプライアンスのトリガーをすぐに検出できます。これは、組織のセキュリティを確保する最初の検出方法です。

教師あり学習は、ThreatML の優先順位付けを行う部分です。これは、イベントを検査するだけでなく、関連するすべての周辺データを検査してそのイベントに関する予測を行います。その目的は、「このワークロードの過去の行動から、このイベントが予測可能かどうか」という質問に答えることです。F5 のアプローチは、「観測、検出、認識、反応」というパターンに従っています。

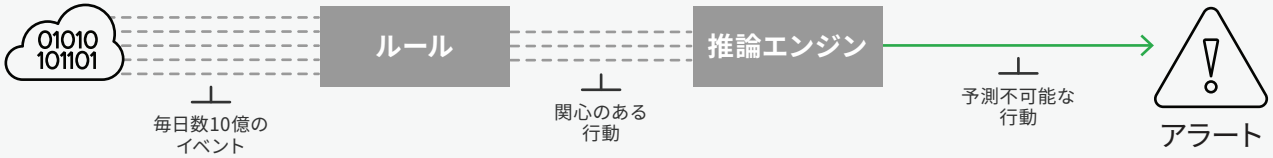

図 1：ThreatML がコンテキストにおける有効性の高いアラートにたどり着くまで

監視する

Distributed Cloud AIP は、コンテナ、Kubernetes、ホストマシンおよびクラウド管理コンソールからデータを取り込み、クラウドスタック全体に及ぶ最も豊富なテレメトリーを収集します。

F5 は、顧客ベース全体で毎日 600 億以上のイベントを処理しています。この幅広いテレメトリー収集は、クラウドセキュリティ監視に対する F5 の包括的なアプローチの基礎となっています。

お客様は**テレメトリー規模**と継続的な**収集**の両方からメリットを得ることができます

お客様は、クラウド環境内のすべての行動を対象とした、このテレメトリーの規模と継続的な収集によるメリットを得ることができます。これは、F5 Distributed Cloud AIP の重要な差別化要因であり、F5 の複数の検出方法の原動力でもあります。

検出

膨大な量のデータから意味のあるセキュリティアラートを表面化させるには、深層検出アプローチが必要です。F5 は、行動ベースのルールと ML 駆動型の検出の両方によりこれを実現します。多くのクラウドセキュリティプロバイダでは、このどちらか一方を選択しなければなりませんが、環境のリスクを正確に検出するためには両方が必要です。F5 Distributed Cloud AIP と ThreatML を利用すれば、その両方を得ることができます。

当社のルールエンジンは、環境における既知の脅威を監視できます。ルールは、システム上で定義した既知の行動パターン内のリスクを捕捉するという点で有益です。一貫した監視は、内部脅威の監視や、コンプライアンス監査時にセキュリティ体制の全体像の把握に不可欠です。

また、教師あり機械学習による検知も行います。クラウドセキュリティでこの種のアルゴリズムを使用するには、トレーニングのために毎日何 10 億ものイベントにラベル付けする必要があります。ThreatML の教師あり学習の新しいアプローチでは、収集したすべてのデータに対してルールエンジンを使ったリアルタイムのラベル付けを行います。これにより、ThreatML は、検出されるすべての行動を監視して、予測できます。

ルールと機械学習により、既知の脅威と未知の脅威の両方を検出し、偽陰性、つまり実際には悪意のある正常な動作を排除できます。

認識

教師あり学習を活用した ThreatML は、適切な行動を迅速に取れるようにすることで平均認知時間（MTTK）と平均応答時間（MTTR）を改善する F5 のアプローチです。その目的は、組織にとって最も重要な行動のみを表面化させることで、すでに負担がかかっているセキュリティチームの運用負担を軽減することです。

ThreatML は、F5 の推論エンジンであり、ルール照合から取得したラベル付きデータにより予測型のモデリングを行います。教師あり学習は、このデータを利用して、周囲イベントが予測可能な行動を示しているかどうかを判断します。このエンジンが予測不可能な行動を発見した場合、ThreatML は、対処が必要な関連するコンテキストとともに、優先順位の高いアラートとして表面化させます。

F5 は、業界をリードするテレメトリー収集と独自の社内データプラットフォームにより、環境に関する行動ベースのセキュリティとリスク予測を行い、リアルタイムで、つまりビジネスにとって最も緊急なアラートに対するより積極的な対処を可能するという一意な立場を確立しています。これは、サードパーティのデータウェアハウスを利用してデータの保存と分析を行うためにリアルタイム性が損なわれることが多い他のベンダーにはない、重要な利点です。さらに、教師あり学習、完全なセキュリティ対象範囲、および深いテレメトリー収集とルールセットの裏付けにより、ビジネスにおいて最も重要なセキュリティニーズに、自信を持って対処できます。

対応

どんなに優れたルールと ML 技術のセットでも、人間の直感、推論、意思決定のスキルに置き換わることはできません。F5 のアプローチは、ルールと教師あり学習を組み合わせてアラートの量を減らすことで、最も重要な行動の脅威だけに焦点を当てることができるようにします。F5 のプラットフォームは、スタック全体を対象として、ノイズから関連行動を選別し、注意が必要な優先順位が最も高いアラートのみを表面化させるという難しい作業を行い、最終的に MTTK や MTTR などの主要メトリクスを改善します。

また、F5 の 24 時間 365 日体制の SOC チームがセキュリティの専門知識をご提供し、日々のセキュリティ運用をサポートいたします。さらに、F5 Distributed Cloud AIP Managed Security Services は、F5 の広範なテレメトリー収集と教師あり学習も利用しながら、お客様に代わり、重大度の高い問題の検出とトリアージを行い、アラートを調査できます。

F5 セキュリティ専門家がお客様と連携すればするほど、お客様側で行われる行動が ThreatML のモデルに反映されます。時間の経過とともに、F5 はインフラストラクチャのどの部分が特定のビジネスにとって最も重要であるかを理解できるように進化していきます。その結果、お客様はアラートが脅威となる前に、環境内で優先順位が最も高いアラートに集中いただくことができます。

クラウドセキュリティの未来は教師あり学習

F5 Distributed Cloud AIP、特に ThreatML は、お客様のペインポイントと価値への対応に尽力していることを証明し続けています。F5 は、セキュリティ専門家が最終的にその環境内のリスクを管理できるようサポートするために、サイバーセキュリティソリューションを可能な限りプロアクティブかつ効率的にすることに取り組んでいます。F5 は、テレメトリー収集とデータプラットフォーム、ルール、進化する ML などを重要な基盤として、検出を犠牲にすることなく、最も関連する実用的なアラートを提供し続けています。

テレメトリー収集や**データプラットフォーム**、**ルール**、**進化する ML** などを重要な基盤として、関連する実用的なアラートを提供します。

F5 は、常に現状を打破し、革新により問題を解決して、お客様が組織内でより大きな価値を推進できるようにサポートすることをお約束します。教師あり学習を利用した ThreatML は、クラウドセキュリティにおける大きな一歩です。他の企業が追いつこうとする一方で、F5 はイノベーションを継続し、クラウドセキュリティをさらにイノベーションして参ります。ぜひご期待ください。

付録

[1]「人材へのアクセスがマネージド・サービスの機会を促進する」451 Research（https://go.451research.com/2020-miaccess-to-talent-driving-managed-service-opportunity.html）

[2]「IDC FutureScape：2020 年世界のクラウドの予測」IDC（https://www.idc.com/research/viewtoc.jsp?containerId=US44640719）

THREAT STACK：F5 ソリューションになりました

Threat Stack は製品名称を変更し、F5 Distributed Cloud App Infrastructure Protection(AIP) となりました。本ソリューション、F5 セキュリティオペレーションセンター（Distributed Cloud AIP Managed Security Services、Distributed Cloud AIP Insights を含む）、およびその他について詳しくは、F5 のクラウドセキュリティとコンプライアンスの専門家までお気軽にお問い合わせください。

クラウドセキュリティのお悩みは F5 セキュリティ専門家にぜひ任せください。詳細およびデモのご予約については、F5 のウェブサイトをご覧ください。

©2023 F5, Inc. All rights reserved.F5 および F5 のロゴは、米国およびその他の国における F5, Inc. の商標です。その他の F5 の商標は、f5.com に記載されています。
ここに記されているその他の製品、サービスまたは企業名は、各所有者の商標である可能性があります。F5, Inc. は明示的にも暗黙的にも承認または提携を主張していません。
DC 12.22 | JOB-CODE-EBOOK-950840192-ThreatML-Supervised-Learning