ホワイトペーパー

セキュリティ

SOC における機械学習

データの増加、攻撃経路の高度化、リソースの減少、複雑なセキュリティツールエコシステムなど、今日のセキュリティオペレーションセンター (SOC) を取り巻く状況は悪化しているように見えるかもしれません。異常検出と教師なし機械学習は、SOC チームの生産性の回復と脅威検出の改善を促進し、次世代のセキュリティオペレーションを強化します。

MICRO FOCUS

目次

ページ

こうした「未知の」脅威に対抗するには、機械学習を活用した、より高度な脅威検出アプローチが必要です。

はじめに

今日のセキュリティオペレーションセンター (SOC) は、かつてないほど大きな課題に直面しています。SOC チームは、ますます高度になる脅威を、短時間でより多く検出するように迫られています。もはや人間の力だけでは対処できない領域です。

現代の SOC では、相関を活用するルールベースのセキュリティツールが重要な役割を果たしています。セキュリティチームは既知の攻撃パターンを手がかりにして、迅速に脅威を検出します。しかし、非常に複雑な一部の脅威は、明確な証拠を残さず、過去に例もないため、検出の網をすり抜けてしまうことがあります。こうした「未知の」脅威に対抗するには、機械学習を活用した、より高度な脅威検出アプローチが必要です。

本書では、セキュリティチームが機械学習を活用した異常検出を駆使してセキュリティオペレーションを強化する方法について解説します。また、ソリューション選択のベストプラクティスを提示し、SOC で機械学習を最大限活用するためのガイダンスを提供します。

機械学習と異常検出

セキュリティ上の深刻な脅威に関するヒントは、膨大なデータの中に埋もれています。雑音を取り除いてそのヒントを見つけることは、針の山から 1 本の針を見つけるようなものです。ここで、機械学習を活用した異常検出が大きな効果を発揮します。膨大な量のデータを迅速に分析し、重要な脅威を絞り込む異常検出によって、SOC チームにおける脅威の検出、トリアージ、調査、対応の効率と速度を高めることができます。

サイバーセキュリティにおいて一般にユーザー / エンティティ行動分析 (UEBA) と呼ばれるこのテクノロジーは、数百種類の機械学習モデルを活用して膨大な量のイベントを分析し、組織内のあらゆるエンティティ (ユーザー、マシン、プリンタ、IP アドレスなど) の「通常」の行動を明確にします。このベースラインに基づいて、そのエンティティについて得られた新たな情報の潜在的なリスクを評価します。エンティティごとに、ベースラインを新たなアクションや他のベースラインと比較してリスクスコアを生成し、数百個のヒントの間の点をつないで、通常とは異なる行動が実際にセキュリティリスクなのかどうかを評価します。このように、多数のデータポイントをより危険度の高い少数の脅威リードに変換してアラートを減らすことにより、SOC アナリストは組織に実際にリスクを及ぼす脅威の検証に集中することができます。

適切なツールの選択

たとえば、インサイダー脅威や標的型の外部攻撃は複雑なため、効果的に検出するには異なる種類の機械学習が必要になります。

人工知能 (AI) と機械学習はあらゆるベンダーが採用していますが、購入する側は、望む価値が得られるソリューションを容易に選別できない状態です。

サイバーセキュリティで最も一般的な機械学習の種類は、いわゆる教師あり機械学習です。この場合は、ラベル付けされた膨大なデータセットを使用してモデルをトレーニングする必要があります。この手法は、既知の攻撃パターンやセキュリティ侵害インジケーター (IOC) を持つ既知のサイバーセキュリティ脅威を特定するのに適しているため、広く普及しています。たとえば、マルウェア検出は、この種の機械学習に最も適した使用事例と言えます。業界はマルウェアについて数十年分のデータを蓄積しており、そのデータをモデルのトレーニング教材として使用できるからです。

しかし、すべての脅威にきちんとラベル付けされたデータセットがあるわけではありません。たとえば、インサイダー脅威や標的型の外部攻撃は複雑なため、効果的に検出するには異なる種類の機械学習が必要になります。こうした脅威には、教師なし機械学習の方が効果的です。つまり、ラベル付けされていないデータセットからパターンを導き出す種類の機械学習です。

さまざまな機械学習の種類

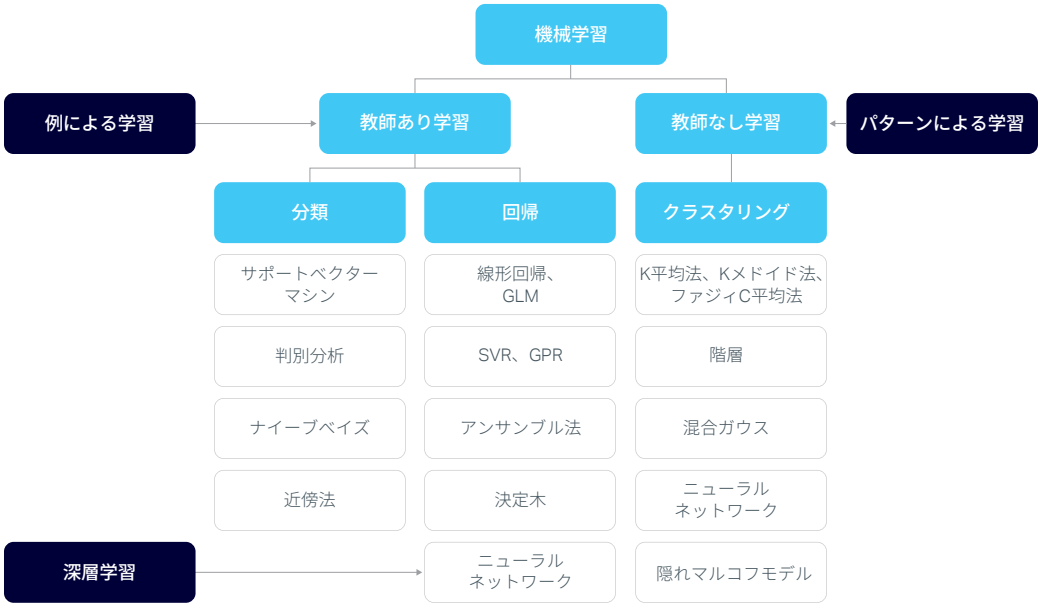

図 1.2 つの異なる機械学習の種類の簡略図：教師ありと教師なし。*(出典：MathWorks with additions by Stephan Jou、Micro Focus® Interset CTO)*

教師なし機械学習は、データセット内のパターンを取得して学習するため、行動を自動的に比較して通常とは異なる行動を絞り込む異常検出に適しています。

教師なし機械学習は、データセット内のパターンを取得して学習するため、行動を自動的に比較して通常とは異なる行動を絞り込む異常検出に適しています。さらに、この種類の機械学習を「オンライン」またはファイアウォール内の環境で実行することにより、何を探すべきか人間が指示しなくても、機械が企業のデータに適合し、新たなパターンを発見します。これは、組織や脅威の変化に応じて人間による設定が必要になるルールベースのソリューションやしきい値ベースのソリューションとは異なります。

このアプローチは、従来のルールベースの検出テクノロジーのレーダーにかからなかった脅威も漏らさず特定できるため、脅威検出が強化されます。こうした脅威は、決して少なくありません。大企業では、一度に複数の複雑なセキュリティ事例に対処することも珍しくありません。図 2 に示したような、幅広い高度な脅威の戦略とテクニックを検出する必要があります。

防御回避	持続型	実行
通常とは異なるファイルまたはデータアクティビティ 通常とは異なるプロセスアクティビティ 通常とは異なるプロセス関係	休眠アカウントによるアクティビティ 通常とは異なるログオンアクティビティ 通常とは異なるレジストリ変更	通常とは異なるポートまたはプロトコル 通常とは異なるプロセスアクティビティ 通常とは異なるネットワークアクティビティ
権限昇格および認証アクセス	**検出およびラテラルムーブメント**	**収集および持ち出し**
通常とは異なる認証またはアクセス 通常とは異なるファイルまたはデータアクセス 通常とは異なる PowerShell アクティビティ	めったにないエンティティへのアクセス 通常とは異なる認証またはアクセス 通常とは異なる HTTP トラフィック	通常とは異なるファイルアクセス 通常とは異なるポートまたはプロトコル スクリプトまたはボット的なアクティビティ

図 2. Interset UEBA などの教師なし機械学習による異常検出で発見された MITRE ATT&CK の脅威の戦術および関連する攻撃行動指標の例。

しかし、購入する側は注意が必要です。図 1 のように、このアプローチでは複数の機械学習アルゴリズムが想定されます。組織のあらゆるセキュリティニーズを満たす万能薬的な 1 つのアルゴリズムは存在しません。深層学習、ニューラルネットワーク、ベイジアンメソッドは、いずれも広く注目されていますが、実際の作業に適したアルゴリズムは、SOC が処理するデータセットと想定される使用事例によって異なります。

SOC における機械学習のベストプラクティス

機械学習にはセキュリティオペレーションを変革する力がありますが、他のパワフルなテクノロジーと同様に、戦略的に選択して導入する必要があります。機械学習で最適な結果を得るための 4 つの重要な要素について考えてみましょう。

1. 使用事例からスタートする
問題を把握しない限り、解決策を見つけることはできません。新たな機械学習テクノロジーを購入または導入する前に、組織にとって最も重要なセキュリティの使用事例を明確にします。解決しようとしている問題を把握して明確化したら、そのニーズに最適なテクノロジーを選択する段階に入ります。

2. バズワードの罠にはまらない
AI や機械学習はサイバーセキュリティではおなじみの用語ですが、こうしたテクノロジーの採用を主張しているベンダーをすべて信用できるわけではありません。ベンダーのソリューションでどのような機械学習が使用されているのか、またその機械学習が自分のセキュリティチームのニーズに適合するのかを検証する必要があります。データサイエンティストになる必要はなく、機械学習の仕組みについて少しだけ理解することで、ベンダーを評価する際に効果的に質問できるようになります。たとえば、「既存のツールやテクニックで検出できないのはどのような脅威ですか？」と、「貴重な情報が含まれているのに現時点で十分に活用できていないデータフィードはどのようなものがありますか？」といった質問が考えられます。

3. 機械学習は万能薬ではない
最適な防御のためには、できるだけ多くの拠点を防御する必要があります。機械学習だけが悪意のある攻撃者を見つけて阻止するのではありません。パワフルな UEBA と次世代の SIEM を組み合わせることで、多層的なセキュリティ分析アプローチが得られます。可視性と検出能力が高まり、既知の脅威にも未知の脅威にもすばやく容易に対応できるようになります。リアルタイムの相関付けによって既知の脅威をすばやく効果的に見つけ出し、UEBA によって検出の網をかい潜る狡猾な脅威を検出します。現実的な脅威のシナリオでは、多くの場合、この両方のアプローチを組み合わせる必要があります。

4. 人間と機械のチームを作り上げる
SOC の人員はこれまで以上に貴重な存在ですが、彼らは困難な課題に直面しています。あらゆる SOC チームは、雪だるま式に膨れ上がるデータフィードと、絶えず進化する脅威への対処に苦慮しています。予防的なセキュリティ警戒体制は、人間と機械のそれぞれの強みを活かしたチームによって生まれます。機械は、人間にはできないスピードで分析を行い、リードを発見します。SOC アナリストとスレットハンターは、そのリードを調査し、コンテキストを把握します。

パワフルな UEBA と次世代の SIEM を組み合わせることで、多層的なセキュリティ分析アプローチが得られます。可視性と検出能力が高まり、既知の脅威にも未知の脅威にもすばやく容易に対応できるようになります。

重要な脅威を検出する準備は万全ですか？

保護すべき貴重な資産を保有する企業、セキュリティまたは財務リソースが限られている企業、監視範囲が広大な企業にとって、機械学習は、予防的アプローチによる効果的なセキュリティを確保する上で大きな意味を持ちます。SOC チームは、貴重な時間を手作業や誤検出の検証に浪費することなく、より多くのデータを分析し、迅速かつ効率的に脅威を検出して、早期に修正作業に着手できます。詳しくは、**microfocus.com/ja-jp/interset** をご覧ください。

詳細情報はこちら：
www.microfocus.com/interset

お問い合わせ先：
www.microfocus.com

マイクロフォーカスエンタープライズ株式会社
jp-info-enterprise@microfocus.com
www.microfocus-enterprise.co.jp