セキュリティ分析および UEBA のバイヤーズガイド

本文書は、セキュリティチームがサイバーセキュリティのためのユーザー / エンティティ行動分析 (UEBA) を比較および最終的に購入するプロセスにおいて、情報提供依頼書 (RFI) および提案依頼書 (RFP) を作成する場合のガイドとして作成されました。

ガイド

www.microfocus.com

バイヤーズガイド

セキュリティ

MICRO FOCUS

目次

既存のセキュリティツールの機能を補完してリスクの可視性を向上する

セキュリティ分析は、以下の機能を提供することで、既存のセキュリティツールにおけるリスクの可視性と ROI (投資収益率) を向上します。

1. 既存の断片的なツールを上回る水準でリスクを可視化します。
2. 脅威のヒントに優先順位を付けることで、セキュリティチームの悩みの種となる膨大なノイズと誤検知を削減します。
3. 直感的なクリックスルー型のインターフェイスでコンテキストと未加工のイベントにアクセスできるため、インシデントの調査と根本原因の分析をスピーディに行えます。その結果、調査時間、各インシデントを担当する FTE 調査員の数、そして外部コンサルタントの採用関連コストを削減できます。
4. 脅威とリスクに自動的に優先度が設定されるため、既存のセキュリティ投資の効果が向上します。具体的には、セキュリティ情報 / イベント管理 (SIEM) システム、マルウェア脅威検知ツール、エンドポイントの検知と対応 (EDR)、エンドポイントプラットフォーム保護 (EPP)、およびネットワークデータ損失防止 (DLP) テクノロジーへの投資が対象になります。
5. 教師なしの機械学習により、運用コストを削減しながら、通常および異常な行動を広範囲で統計的に自動測定し、複雑なしきい値ベース、ルールベース、およびポリシーベースの運用管理から解放します。

本文書は、セキュリティチームがサイバーセキュリティのためのユーザー / エンティティ行動分析 (UEBA) 製品を比較および最終的に購入するプロセスで情報提供依頼書 (RFI) および提案依頼書 (RFP) を作成する際に役立つガイドとして作成されました。本文書は 5 つのセクションで構成されます。最初に、テクノロジーを導入する十分な理由をお示しし、次に包括的なセキュリティ分析製品に不可欠な機能を定義します。

付録として、製品の選定に役立つチェックリストと比較チャートをご用意しています。

データソースとリスク対象

「見えないものは止められない」ということわざは、セキュリティ分析製品にも如実に当てはまります。リスクの可視性は、利用するデータソース次第で変わります。仮に、エンドポイント、セキュリティ侵害を受けたアカウント、アプリケーション、リポジトリに格納されたデータに対して同時に攻撃が仕掛けられたとします。この場合、データ窃盗犯はデータをサーバー内でステージングした後、ひそかに盗み出します。このような攻撃に対してセキュリティ侵害インジケーター (IOC) の全体像を詳細に把握するには、関連する各資産に格納する数種類のログデータを調査することが不可欠です。1 種類または 2 種類の資産のログだけを調査する場合、攻撃は検知できても、識別や阻止まではできない可能性があります。過去の攻撃事例を振り返ると、こうした問題が広く見受けられます。セキュリティ分析製品がエンドポイントのアクティビティ、Active Directory (AD) ログ、IP リポジトリログ、そしてサーバーログを収集している場合、分析エンジンが攻撃を特定および関連付けて明確化し、通知を送信し、ライフサイクル全体を可視化します。

ツールの評価時には、各ツールが使用するデータソースの範囲を第一に検討する必要があります。セキュリティ分析製品の多くは、SIEM 製品が収集したメタデータとログデータを利用する、または AD や他の LDAP (Lightweight Directory Access Protocol) のディレクトリストア内のデータを特定およびアクセスできます。これらのデータソースを調査の第一歩と位置付けることは間違いではありませんが、上記の攻撃への対策としては不十分です。これらのセキュリティ分析製品の中で明確な差別化要因となるのは、利用するデータストアやデータソースの数と種類です。長期的にリスクの可視性を最適化するために、社内のインフラストラクチャに適合する広範なデータ収集セットを探しましょう。

別の重要な考慮事項として、複数のモデルを活用してより良質なコンテキストを取得できるように、複数のデータソースを自動的に関連付けて分析精度を向上させる機能が分析エンジンに備わっているのか、そしてその場合にどのような手法が採用されているのかを検討しましょう。データセットを結合すれば、複数種類の証拠を組み合わせることができます。その結果、検知の正確性、適時性、コンテキスト精度が向上します。たとえば、セキュリティ侵害を受けたアカウントが異常なプロセス処理 (エンドポイントデータ) を実行し、疑わしい DNS クエリ (ネットワークデータ) を出し、さらにネットワーク共有に異常なアクセス履歴 (サーバーアクセスデータ) が見受けられる場合があります。数学的に正確な全体像を描くには、データフィードを適切に関連付けて、検出した攻撃ステップを総合的なリスクスコアに集約し、関連するアクティビティを該当するすべてのエンティティ (アカウント、マシン、ファイル、アプリケーション) で表示する必要があります。

データソースを理解する

SIEM データ

SIEM はオリジナルのデータソースではなく、ユーザーディレクトリ、サーバーログ、セキュリティツールから多様なセキュリティデータを収集しています。他のデータソースと異なり、SIEM データの大きな利点は、すぐにデータを入手してセキュリティ分析製品に読み込めることです。分析エンジンでこのデータを分析すれば、ユーザーアクセスやアクティビティイベントの情報を元に内部ユーザーによる攻撃を割り出せます。同様に、境界防御および NetFlow のデータを組み合わせて分析することで、マルウェアやアカウント乗っ取り攻撃も検知できます。しかし、市場で導入済みの SIEM の大半は、システムの膨大なコストが足かせとなり、限られたシステムログしか収集できていません。また、サーバー、あるいは基幹的な役割を果たすエンタープライズアプリケーションやリポジトリからデータを収集しているケースはほんの一握りです。SIEM データは素晴らしい出発点なのですが、多くの場合、SIEM で収集されるログは高度な攻撃を可視化するには不十分です。

ディレクトリデータ
AD および LDAP ディレクトリの情報は、セキュリティ分析製品で最も広く利用されているデータソースです。役割、組織、アクセス権を把握できるだけでなく、すべての情報をベースラインとして使用できます。認証イベントを含むディレクトリデータを使用すれば、アカウント侵害を効果的に検知することができます。単一のデータソースを利用する場合は誤検知になるケースが圧倒的に多いのですが、サーバーへのアクセスデータを分析対象に含めれば、内部ユーザーによる攻撃を一定程度効果的に検知できます。

VPN、プロキシ、NetFlow
ネットワーク通信のデータを収集するセキュリティ分析製品を導入すれば、組織内のネットワークに侵入する高度な攻撃を可視化しやすくなります。このデータには、データの転送量、データの転送場所、マシン間の異常な接続、異常な内部または外部ソースへの通信などの情報が含まれます。ネットワーク情報は内部ユーザーによる攻撃を一定程度検知できますが、極めて限定的なコンテキスト下での運用であり、ネットワーク外のマシンには対応できません。NetFlow データは、外部の Web サイト、コマンド、および制御呼び出しと通信する際の異常値を探し出し、外部からの攻撃を検知できます。また、通常とは異なる大規模なデータ移動も簡単に検知できます。

エンドポイント
セキュリティ分析の分野で、エンドポイントのデータを収集しているベンダーはごく一部です。他のベンダーは、直接または SIEM 経由で、既存のエンドポイント (例：DLP または EDR) からデータを取得し、利用しています。エンドポイントのデータは、オンラインとオフラインの両方で、ユーザーのアクティビティだけでなく、アプリケーションやネットワーク、クラウドのアクティビティも豊富に含んでいます。マルウェアベースの攻撃や内部ユーザーによる攻撃を判断するためのコンテキスト情報を提供します。この情報には、ファイルアクティビティ (印刷、コピー、送信、ダウンロード)、デバイスアクティビティ (USB またはブルートゥースのアクティビティ、コピー、ダウンロード)、アプリケーションアクティビティ、さらには多様なネットワーク通信が含まれます。

データ /IP リポジトリのログ
データ /IP リポジトリのデータを利用するベンダーは少数ですが、この取り組みは高度な標的型攻撃や内部ユーザーによる攻撃をコンテキスト化するうえで極めて重要です。セキュリティ分析製品でソースコード管理や製品ライフサイクル管理、電子コンテンツ管理を通じて、または SharePoint などの広範なリポジトリからデータフィードやログデータをリアルタイムで活用すれば、エンタープライズ内の脅威に対して卓越した可視性を発揮できます。ソースのログデータ (例：タイムスタンプ、ユーザー、IP アドレス、アクション、リソースパス) から少数の列セットを取得するだけで、重大な脅威に関するコンテキストを収集できます。このコンテキスト情報には、退職者による社外への機密データの持ち出しや、データをひそかに盗み取ろうとする攻撃者の検知も含まれます。イベント情報は豊富に存在しますが、ハードウェア費用とネットワーク費用を削減するために IT 部門がログ記録システムを有効化しないケースが多いため、このようなデータの収集は困難です。IP 保護に真剣に取り組む企業は、こうしたシステムを自社のセキュリティ分析製品と組み合わせて活用する必要があります。

ERP/ エンタープライズアプリケーションとデータベース
セキュリティ分析の分野で重要なデータソースは他に 2 種類あります。1 つ目は、主要なエンタープライズアプリケーションである SAP や Oracle などの運用システムが格納するログデータとアクセス制御データです。このデータを収集すると、コンテキスト性が向上するとともに、ビジネスプロセスや財務データ、人事記録に対する攻撃も可視化しやすくなります。2 つ目は、構造化データ (SQL データベース) です。識別情報を収集することで、(PII および PHI データベース内の) 機密データに関してコンテキスト情報を提供します。これらのシステムに格納するログデータを利用することで、内部ユーザー (とりわけ特権ユーザー) による攻撃や、標的型のアカウント乗っ取り攻撃を検知しやすくなります。

データのエンリッチメント
セキュリティ分析ツールの効果を向上する新たなデータを組織内で生成したり取得できます。分析定義インシデントデータとその他のデータ (ウォッチリスト、脅威インテリジェンスフィード、セキュリティアラート、ガバナンス、制御ツールなど) を関連付けると、インシデントに関するコンテキスト情報が生まれ、検知速度が向上します。エンリッチメントデータを使用することで、分析スコアの高低の調整や、エンリッチメントツールで定義した特定のイベントの呼び出し / 通知を行えるほか、インシデントのコンテキスト情報を追加することで調査中の攻撃の全体像を把握しやすくなります。

証拠として収集するデータセットの種類が大きくなるほど、すばやく正確により多くの脅威を特定できます。脅威を検知するためには、単一データソースのデータ量でよりも異なるデータソース内のデータ量が重要になります。

バイヤーズチェックリスト：データソース
- ❑ データフィードの関連付け (複数のフィードを関連付けてエンティティ全体の相対的なリスクを把握する)
- ❑ SIEM から取得するデータ
- ❑ AD および他の LDAP ディレクトリストアから取得するデータ
- ❑ 認証およびアクセス試行
- ❑ HP ArcSight、McAfee ESM、IBM QRader などのシステム内に格納する AD のイベントログ
- ❑ Windows セキュリティイベント
- ❑ ファイル共有システム、データベースシステム、ソースコードシステム (例：Perforce、GitHub Enterprise) やその他のリポジトリログなどの知的財産やデータリポジトリから取得するデータ ≤ NetFlow などのネットワークフィードやネットワークタップから取得するデータ

- ❑ エンドポイントから取得するデータ
- ❑ オペレーティングシステムや、サーバー、エンタープライズアプリケーション、アクセス制御リスト (ACL)、費用、電子メール、ファイル共有、Web プロキシ、プリンターログなどのマシンおよびシステムから直接取得するデータ
- ❑ データエンリッチメントソース
- ❑ セキュリティツールアラート (DLP、NAC、GRC)
- ❑ 脅威インテリジェンスフィード
- ❑ ウォッチリスト (ユーザー、実行可能ファイルなど)

数学的手法：機械学習と行動分析

セキュリティ分析ソリューションの目標は、組織内の脅威、とりわけ既存ツールで検知しにくい脅威をすばやく正確に検知することです。行動分析は組織内の各エンティティに合わせたベースラインで測定します。ベースラインの精度を向上して異常なイベントを識別します。そして、これらのイベントを当該イベントに関係するエンティティと関連付けます。エンティティには、ユーザー / アカウント、マシン、アプリケーション、ファイル、その他のデジタル資産が含まれます。エンティティが異常なアクティビティを行うと、確率的手法でそのイベントの異常度が定量化され、適切なリスクスコアが測定されます。このリスクスコアを元に、最初に調査するべきエンティティを割り出し、その優先度をビュー画面に表示します。

機械学習

従来、セキュリティマネージャーは、リスクを定義するために「何 MB の添付ファイルまで許可するか」などハードコードのしきい値を指定する必要がありました。その結果、特定の数字をグローバルかつ広範囲に個人や企業のプロセスに採用することになり、脅威の定義が不安定で実用性を欠くうえに、導入と保守に多額の費用がかかっていました。機械学習では、各エンティティの実情に合わせてデータのベースラインを動的に算出します。たとえば、履歴書を日常的に送信する人事ディレクターと添付ファイルをめったに送信しない契約社員とでは異なる対応を取るべきです。この手法を導入することで極めて正確かつ効果の高い数学的傾向を掴み、組織全体で標準的なベースラインを定義できます。

確率的数学モデル

確率的手法を用いない従来のセキュリティシステムでは、ブーリアン型のルール (適用か不適用かの二択) を使用するため、アラートの生成や管理の軽減を実行するルールやしきい値に依存してしまいます。たとえば、ブーリアン型のルールでデータの移動量が 350GB を超えるとアラートを作動するように設定すると、351GB では作動しますが、349GB では作動しません。ブーリアン型の手法では、ルールの適用にあたり特定アクティビティの異常度を判断できません。あるユーザーが自らの職務を遂行するために平均 380GB のデータを移動する場合にも設定ルールが作動するため、誤検知になります。

一方、確率的数学手法では、たとえば、0% から 100% までの段階的な数値でイベントを測定します。そのため、完全に正常な状態から極めてリスクが高い状態まで幅広く測定できます。この機能により、他の類似イベントと効果的に比較し、その乖離の程度、つまり異常度を測定できるのです。たとえば、通常は平均 15GB のデータを自身のコンピューターからクラウドへ毎日移動するユーザーが、1 時間で 400GB を移動したとします。確率的数学モデルは、通常の行動と極めて異なる行動と判断し、その差異を指摘します。上記の例で確率的モデルは、同じ 400GB 分の送信でも、通常で平均 380GB を送信するユーザーは、通常 15GB しか送信しないユーザーほどのリスクはないと判断します。この分析機能を利用すれば、ルールとしきい値への依存から解放されます。

バイヤーズチェックリスト：高度な分析

- ❑ データフィードの関連付け (複数のフィードを関連付けてエンティティ全体の相対的なリスクを把握する)
- ❑ エンティティ別の対象：ユーザー / アカウント、マシン / デバイス、ファイル / 資産
- ❑ 教師なし機械学習
- ❑ 確率的数学ベースのリスクスコアリングルール
- ❑ 導入後すぐに利用可能な確率的数学モデルを搭載：
  - ❑ 時間
  - ❑ ボリューム
  - ❑ ソース
  - ❑ 送信元 / 送信先
  - ❑ ユーザー
  - ❑ 統計的ピアグループ
- ❑ エンティティからイベントへ、イベントからエンティティへ関連付けるリスクスコアリング
- ❑ 導入後すぐに利用可能で、脅威に対応する複数の確率的数学モデル (ベイズモデル、クラスタリング、ニューラルネットワーク、ロジスティック回帰分析など) を活用して以下を検知可能
  - ❑ アカウントの悪用
  - ❑ セキュリティ侵害を受けたアカウント
  - ❑ コマンドアンドコントロール (C2：指揮・統制)
  - ❑ データステージング
  - ❑ データ窃盗
  - ❑ 内部ユーザーによる脅威
  - ❑ 内部スパイ
  - ❑ 感染したホスト
  - ❑ ラテラルムーブメント (侵入後の攻撃)

インシデントの対応と調査

インシデント対応にセキュリティ分析を導入する目的は、脅威を明確かつ正確に識別および特定することです。脅威に関する実用的なデータをセキュリティチームに提供することで、データ侵害を未然に防げます。以下の要件を満たすセキュリティ分析製品を選定することが重要です。

使いやすさ

セキュリティツールでは、複雑なインターフェイスが足かせとなり、最大級のリスクの所在や、そのリスクのコンテキストを表示できていません。一方、ダッシュボードでは、リスクの高い IP アドレスや疑わしいマルウェアシグネチャに対して、イベント数や長期的な変化量、単一イベントの追跡記録を表示できます。セキュリティツールの使用法を習得するには、数日から数週間かかるのが普通です。高度な分析を実施すると、ユーザー / アカウント、マシン、アプリケーション、ファイル、デジタル資産といったエンティティ内で「何が」関与しているのかを簡単に表示できます。その分析結果に優先度を付けることで、セキュリティマネージャーは、どのインシデントが最大のリスクか、次に重大なリスクは何か、などをすばやく識別できます。

インシデントのコンテキスト情報

リスクに優先度を付けた後に、調査員が 1 回クリックするだけでインシデントのコンテキスト情報を画面に表示させる機能が必要です。コンテキスト画面は、どのエンティティ (ユーザー / アカウント、マシン、ファイル、場合によってはアプリケーション) が関与しているかを直ちに明示するものでなければなりません。また、そのインシデントの異常度も表示するべきです (移動するデータの機密性、移動するデータ量、アクセスされたデータの格納場所、関連する実行可能ファイルの種類、アクティビティの時間など)。明瞭な表現と分かりやすいグラフで情報を伝達することで、特別なトレーニングは不要になります。その結果、レベル 1 の SOC アナリストでもツールを効果的に活用して脅威を識別および検証し、適切に対処できます。

インシデントに対する実用的なフォレンジックとエクスポート

インシデントの発生後ではなく、発生中に検知する場合、いかに速くフォレンジック調査と被害軽減策を実施できるかが鍵を握ります。インシデントを迅速に検証してインシデント対応プロセスに移行するために、セキュリティ分析製品には攻撃を定義するイベント単位で証拠を提供することが求められます。攻撃のライフサイクル全体を簡単に調査およびエクスポートする機能が必要です。その対象は、エンドユーザーのマシンで実行する動作の詳細 (アプリケーション、ファイル、ファイルアクティビティ、切り取り、コピー、貼り付け、同期、クラウド) から、IP などの機密データが脅威にさらされているネットワーク全体で攻撃がどのように展開しているかまで多岐にわたります。調査チームに対して、内部ユーザー、侵害を受けた複数のアカウント、感染したマシン、および不正アクセスを受けたリポジトリ間での共謀攻撃など、インシデントの証拠を実用的な水準で詳細を添えて提供することが求められます。

セキュリティチームが SIEM を導入中の場合、関連するエンティティにイベントの証拠を紐付けることで価値が生まれます。これは、SIEM では通常このような情報は提供されないためです。お使いのセキュリティ分析ツールから SIEM へインシデントのデータを自動送信することで、インシデント対応の質が飛躍的に高まります。セキュリティチームが SIEM 製品を導入していない場合は、セキュリティ分析製品がこの機能をインシデント対応プロセスの一環として提供する必要があります。その結果、調査員はインシデントに関するアラートを受けてリスクを認識した後に、インシデントのコンテキスト把握、イベントへの詳細なフォレンジック、さらには自由形式の調査をすみやかに実施できます。証拠を収集後、セキュリティ分析製品にはその証拠を SIEM の枠を越えて、ケース管理や証拠フォレンジックに対応する製品へエクスポートする機能が求められます。

インシデント対応プロセスの統合

ここで紹介する機能は、初期の調査 / 検証用のインシデントフォレンジックとは異なります。これらの機能はプロセスに関連するものであり、重要なのは検知時には攻撃が進行中であるということです。このため、迅速な対応が不可欠です。すべての企業のセキュリティチームにおいて、異なる種類のインシデントに備えて適切なプロセスを定義するインシデント対応の戦略ガイドが必要です。その中には、インシデント対応チームへの通知、セキュリティ部門以外 (法務、IT、人事、PR など) への通知、手動対応プロセスの有効化、さらには DLP、アクセス制御、およびその他のセキュリティツール内でのダウンストリーム IT 制御の自動化なども含まれます。浮上した脅威とインシデントデータをインシデント対応プロセスおよびツールに統合するために、インシデントの初期ソースとして、セキュリティ分析製品に統合ワークフローと REST API (Representational State Transfer Application Programming Interface) を組み込むことが重要です。

ワークフローシステムには、テキストやメール、スケーリング、さらにはエンタープライズ内のインシデント対応チームに所属するユーザー数十名を対象とする自動通知機能が必要とされます。また、ワークフローシステムには、インシデントのプロセス内の各段階で柔軟に動作し、異なるインシデント変数に対応することが求められます。たとえば、リスクスコアが 60 を超えるとセキュリティチームまたは SOC 調査員に通知し、リスクスコアが 80 を超えるか、ウォッチリスト内のユーザーであると特定した場合はインシデント対応チームの全員に通知するような機能が必要です。地理、ユーザーグループ、またはファイルの種類に関連するアクティビティに合わせて、通知の精度を向上することも重要です。

API の統合は、インシデント / イベントの証拠をフォレンジック調査ツールへエクスポートしたり、ダウンストリーム型の自動 IT 制御を有効化するうえで極めて重要です。セキュリティチームが SIEM データをセキュリティ分析製品に送信して分析し、SIEM ツールに戻すことを希望する場合もあります。また、ネイティブのアウトバウンド統 合 (例：Phantom、Open DXL、JIRA お よ び ServiceNow へ の

REST 呼び出し) では、攻撃の展開前にセキュリティチームが数時間の猶予を持てるため、対応を自動化できます。ワークフローがフォレンジックデータとしてプロセス内で機能し、浮上した特定のインシデントに合わせて制御が有効化されます。

バイヤーズチェックリスト：インシデントの対応と調査

- ❑ インシデントダッシュボード
- ❑ リスク別のインシデント優先度 ≤ インシデントのコンテキストビュー
- ❑ イベントレベルのインシデントフォレンジックと自由形式の調査
- ❑ ワークフローでのインシデントのやり取り
- ❑ script/API 呼び出しとのワークフロー連携
- ❑ SIEM 統合
- ❑ REST API

ビッグデータのアーキテクチャと導入

ビジネスインテリジェンス (BI) 分野や小売の Web 市場における分析技術の成功事例を見ると、システムが分析する取引データとプロセスデータが大規模であれば価値を創出できる点を踏まえることの重要性が分かります。これはビッグデータにも当てはまります。また、セキュリティ分野の分析でも同様です。単一の IP リポジトリからユーザーやアプリケーションのイベントを収集するだけでも、1 ヵ月で簡単に数十億件のイベントデータを取得できます。複数のソースを追加すると、数日、場合によっては数時間で数十億件のイベントに達します。セキュリティ分析製品のアーキテクチャをビッグデータ環境に対応させる必要があります。ビッグデータ、データウェアハウス、およびデータ管理分野では、Cloudera、Hortonworks、MapR の名前がよく知られています。このような企業は、比較的規模の大きい企業の BI チーム、そしてクラウドプロバイダーやマネージドサービスプロバイダーに事前定義したビッグデータのインフラストラクチャを提供しています。セキュリティ分析製品は、これらと同じフレームワークに対応しています。

企業の規模が大きくなるほど、共有型プライベートクラウドアーキテクチャ内にビッグデータやデータレイクのインフラストラクチャを導入する傾向にあります。導入済みの場合、その企業のセキュリティマネージャーは、既存のインフラストラクチャを活用して導入プロセスの合理化を図る必要があります。市場ではさらなる価値を創出するためのビッグデータ戦略が求められています。洞察力のあるセキュリティマネージャーは、この要件に対応することで、ビッグデータを活用するセキュリティ分析プロジェクトに必要なリソースと支援を手に入れることができます。ビッグデータ基準に完全対応するセキュリティ分析製品を探しましょう。ビッグデータ対応を謳いながら、実際に運用するには従来型データベース / サーバー用のハードウェアやソフトウェアの追加が必要な製品もあります。注意しましょう。

ビッグデータ戦略を採用しない企業は、HP や Supermicro、あるいはマネージドサービス企業やクラウドサービス提供元のクラウドサービスなど、ビッグデータ用途に最適化したハードウェアを活用することが必要になります。アプライアンスのフォームファクターやクラウドベースの導入に対応する Amazon Web Services、Google Compute Platform、Microsoft Azure などは、市場投入までの時間を短縮化する、調達プロセスが長期的で困難になる事態を避ける、ハードウェアの管理および費用負担を軽減するなどの利点があります。

柔軟な導入と運用

他の重要な評価事項は、セキュリティ分析製品の導入と運用です。「使いやすさ」セクションにあるとおり、多くのセキュリティツールが運用環境での製品管理で大きくつまずいています。そのため、デモは良く見えるが現場では使えないという事態に直面しています。残念ながら、多くの GRC、DLP および SIEM の導入でも同様の結果です。その原因は、企業の運用ニーズを満たすためにルール、ポリシー、しきい値が多くなり、複雑化していることにあります。

製品の導入後にセキュリティチームが「予想外の事態」に陥る可能性を最小限に抑えるには、柔軟に導入および運用できるかを踏まえてセキュリティ分析製品を評価することが肝要です。ビッグデータアーキテクチャの導入決定後は、以下の点を考慮しましょう。具体的には、運用開始までの早さと複雑さ、データソースの統合、機械学習にかかる時間、分析および分析の調整、導入に必要なルール設定、新しい脅威を捕捉するために新たな分析機能を追加する機能、そして小規模で運用を開始して簡単に拡大できる仕様などが該当します。

運用開始の早さとデータソースの統合

機械学習を比較的短期間で完了させるために、SIEM や他のデータソースへのコネクタがログデータ履歴を比較的簡単に導入および収集できるか検証しておきましょう。システムやアプリケーションのログデータが初期データソースに含まれている場合、必ずログデータの記録機能を有効化しておきましょう。製品にエンドポイントエージェントが含まれている場合、エンドポイントエージェントを初期導入時に組み込む必要があるのか、マスターイメージ (gold image) や、リソースの要件とスケジュールに応じて後工程で追加できるのかを確認しましょう。

機械学習、分析、ルールの運用開始

機械学習機能では、スキーマをカスタマイズしたり、ルールやしきい値を設定する必要がありません。機密データや特権ユーザー、リスクの高いプロセスに対応する標準的なベースラインの比重を調整する程度の作業で十分です。優れた機械学習は時間の経過とともにこれらの事項を自動的に定義します。システムに機械学習を導入していない場合は、数年ごとにベンダーと連携して構造とスキーマを定義し、標準的なベースラインを設定することが必要になるかもしれません。

機械学習と同様に、確率的数学ベースの分析も、カスタマイズやルールの定義を不要にします。優れたセキュリティ分析製品とは、データに基づいて自律的に学習する製品です。製品にルールやしきい値を設定してアラートやリスクレベルを作動させる場合、セキュリティチームはこれらのルールがどのような制約をもたらすのか明瞭に把握しておく必要があります。これまで未知または未定義だったアノマリ (異常値) は検知できますか？ルールやしきい値の管理、変更、更新は簡単ですか？新しいルールを追加できますか？ルールが数百件ある場合でも簡単に管理できますか？最後に、真に卓越したセキュリティ分析製品は、内部のデータサイエンスチームが、当該ソリューションで使用した実際の数学モデルを設定および調整したり、独自のカスタムモデルを開発および導入することが可能です。

継続運用

セキュリティ分析製品の運用開始後は、データソース、エンドポイント、および分析手法の対象を広げ、広範囲または新興の脅威を検知することが重要です。導入する製品がこれらの対象を横断して柔軟に拡充できる仕様になっているか、そして拡充する際に必要なコンサルティング要件は何かを判断しましょう。最後に、アノマリを定義するためにカスタムスキーマやルールの作成が必要な場合、長期的な制約要件と管理要件が何かを理解し、機械学習や確率的数学手法による優れた自動化機能を備えた製品と比較検討しましょう。

パフォーマンスとスケーラビリティ

言うまでもなく、セキュリティ分析ソリューションの設計時には規模の拡大を念頭に置いておくべきです。多くの企業では、複数のデータソースを横断して従業員全体でセキュリティ分析を実施することになります。そのため、数十億件のトランザクションが発生し、毎月テラバイト規模のストレージを使用します。これは重要な点です。この点を考慮してゼロベースで設計されたソリューションを選定しましょう。さらに、ソリューションは、迅速に規模を拡大してリアルタイムでデータを処理できるものでなければなりません。この性能により、脅威の検知から実際に脅威が発生するまでの時間を短縮できます。

バイヤーズチェックリスト：ビッグデータの導入と継続運用

- ❑ ビッグデータ、Hadoop ベースのアーキテクチャ
- ❑ ビッグデータのオープンソース基準への準拠
- ❑ データソースの収集要件とイベント要件に対応できる拡張性
- ❑ オンサイトとサードパーティの両方のクラウド導入に対応
- ❑ ベンダーのクラウド導入に対応
- ❑ データソース (SIEM、ディレクトリ、リポジトリなど) を簡単に統合可能
- ❑ 導入後、簡単に新しいデータソースを追加可能
- ❑ 導入時に構築が必要なルールベース型ではなく、機械学習が完全に自動化されている
- ❑ アノマリ検知分析が完全に自動化されており、導入時には構築が不要で、ルールベース型ではない
- ❑ 購入した機械学習と分析モデルの更新がライセンスに含まれている
- ❑ 必要に応じて、既存の分析モデルを簡単に設定および調整可能
- ❑ 時間の経過とともに新しい分析モデルを追加して新たな脅威を検知可能
- ❑ オプションでエンドポイントエージェントを選択可能
- ❑ 標準的な管理ツールでエンドポイントエージェントを導入可能
- ❑ 任意の時点でエンドポイントエージェントを導入可能
- ❑ エンドポイントエージェントはマシンやネットワークに過度な負荷をかけない

付録：バイヤーズチェックリスト総合版

	ベンダー A	ベンダー B	ベンダー C
データソース			
データフィードの関連付け (複数のフィードを関連付けてエンティティ全体の相対的なリスクを把握する)			
SIEM 製品から取得するデータ (コア)			
AD および他の LDAP ディレクトリストアから取得するデータ (コア)			
構造情報と役割情報			
認証およびアクセス試行			
ネットワークフィードやネットワークタップから取得するデータ			
エンドポイントから取得するデータ			
ベンダー提供のエンドポイントセンサー			
ベンダーが既存のエンドポイントエージェントと統合			
IP/ データリポジトリ (PLM、SCM、CMS、ECM、ネットワーク共有) から取得するデータ			
サーバー、エンタープライズアプリケーション、アクセス制御リスト (ACL) から直接取得するデータ			
構造化データソース (SQL など) から取得するデータ			
データエンリッチメントソース			
セキュリティツールアラート (DLP、NAC、GRC)			
脅威インテリジェンスフィード			
ウォッチリスト (ユーザー、実行可能ファイルなど)			
高度な分析			
エンティティ：ユーザー / アカウント、マシン / デバイス、ファイル / 資産			
半教師あり機械学習と教師なし機械学習			
確率的数学ベースのリスクスコアリングルール			
導入してすぐに利用可能な確率的数学モデルを搭載			
時間			
ボリューム			
ソース			
送信元 / 送信先			
地域			
エンティティからイベントへ、イベントからエンティティへ関連付けるリスクスコアリング			
導入後すぐに利用可能で、脅威を検知する複数の確率的数学モデル (ベイズモデル、クラスタリング、ニューラルネットワーク、ロジスティック回帰分析など) を搭載			
セキュリティ侵害を受けたアカウント			
内部ユーザーによる脅威			
コマンドアンドコントロール (C2：指揮・統制)			
ラテラルムーブメント（侵入後の攻撃）			
データステージング			
データ窃盗			
特定エンドポイントに対応するモデル			
EDR			
内部ユーザーによる脅威			

次のページに続く

	ベンダー A	ベンダー B	ベンダー C
インシデントの対応と調査			
インシデントダッシュボード			
リスク別のインシデント優先度			
インシデントのコンテキストビュー			
イベントレベルのインシデントフォレンジックと自由形式の調査			
ワークフローでのインシデントのやり取り			
スクリプト /API 呼び出しとのワークフロー連携			
SIEM 統合—ダイレクト双方向コネクタ			
REST API			
ビッグデータの導入と継続運用			
ビッグデータ、Hadoop ベースのアーキテクチャ			
ビッグデータのオープンソース基準への準拠			
データソースの収集要件とイベント要件に対応できる拡張性			
オンサイトとサードパーティの両方のクラウド導入に対応			
アプライアンスのフォームファクターに対応			
データソース (SIEM、ディレクトリ、リポジトリなど) を簡単に統合可能			
標準的な管理ツールでエンドポイントエージェントを導入可能			
任意の時点でエンドポイントエージェントを導入可能			
エンドポイントエージェントがマシンやネットワークに過度な負荷をかけない			
導入後、簡単に新しいデータソースを追加可能			
導入時に構築が必要なルールベース型ではなく、機械学習が完全に自動化されている			
購入した機械学習と分析モデルの更新がライセンスに含まれている			
必要に応じて、既存の分析モデルを簡単に設定および調整可能			
時間の経過とともに新しい分析モデルを追加して新たな脅威を検知可能			

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