バイヤーズ・ガイド： ネットワーク脅威検出・対応 (NDR)

組織に合ったネットワーク脅威検出・対応 (NDR) プラットフォームを選択すれば、見逃されがちな脅威を適切に検出し、素早く対応できるようになり、より強固なセキュリティ体制を構築することが可能です。

はじめに

世界中の組織が攻撃者によるネットワーク侵入を防ぐことを目的としたソリューションやテクノロジーに投資してきた金額を合計すると、数十億ドルに及びます。それにもかかわらず、執拗な攻撃者は今なお境界の防御をくぐり抜けて、攻撃対象のネットワークにアクセスできています。そのような足がかりがひとたび確立されると、何か月も攻撃者に気付かない可能性があり、データ・アセットの盗難や破損のリスクが高まります。

わかりやすいのが、Marriott International の事例です。同社は 2018 年 9 月に、あるセキュリティ侵害によって 5 億件もの顧客レコードが危険にさらされていたことを発見しました。詳しいフォレンジック分析の結果、同社のネットワークには 2014 年 7 月から攻撃者が侵入していたことがわかりました。実に 4 年もの間、攻撃者のアクティビティが見過ごされていたのです。¹

最近の事例では、2021 年 12 月に Kronos のパブリック・クラウドが受けたランサムウェア攻撃が挙げられます。この攻撃によって、複数の給与システムが停止し、多くの大口顧客にデータ侵害が通知されました。さらに、調査を進めていくと、多くの政府機関や組織も同じくデータ侵害の被害を受けていたことが判明しました。このようなネットワークに対する攻撃の兆候を早期に検出するセキュリティ体制を持たない企業や組織が依然として多いことは、現実的な懸念となっています。

従来のポイントインタイム予防ソリューションは、既知のマルウェアのシングネチャに重点を置く傾向があります。そのようなソリューションも引き続き必要ですが、広範囲をカバーするセキュリティとしては不十分です。こうした従来型のセキュリティ・ツールを補完する目的で、疑わしいアクティビティをリアルタイムで検出して対応するツールの必要性が高まっています。この市場の最前線に立っているのが、ネットワーク脅威検出・対応 (NDR) ソリューションです。

Gartner は、2019 年 2 月の『Market Guide for Network Detection and Response』で、このテクノロジーについて次のように説明しています。「機械学習、高度な分析、ルールベースの脅威検出を組み合わせ、エンタープライズ・ネットワーク上の疑わしいアクティビティを検出するためのツールです。NDR ツールは、生のトラフィックやフロー・レコード (NetFlow など) を継続的に分析し、正常なネットワーク動作を反映したモデルを作成します。異常なトラフィック・パターンを検出すると、NDR ツールはアラートを発行します。NDR ソリューションは、エンタープライズ境界をまたがる垂直型トラフィックの監視に加え、戦略的に配置されているネットワーク・センサーから受信したネットワーク・トラフィックやフロー・レコードを分析して、水平型の通信も監視することができます」²

セキュリティ専門家は、企業は自社のネットワークが既に侵害されていると想定するべきであると指摘しています。脅威検出と対応を適切に行うには、ネットワークの動作を把握することが重要です。サイバー攻撃の多くは、ネットワーク通信を通じてマルウェアを配布し、コマンド・アンド・コントロールを行い、データを流出させます。そのネットワーク層にセキュリティ機能を組み込めば、セキュリティ脅威を早い段階で特定するための「見張り台」を構築できます。適切なツールとネットワーク監視技術があれば、セキュリティ担当者は悪意のあるアクティビティを発見し³、それを軽減する迅速な措置を講じることができます。

本バイヤーズ・ガイドでは、セキュリティに重点を置いたネットワーク脅威検出・対応ソリューションに求められる重要な機能と特性、製品を評価する際にベンダーと話し合うべき事項、および製品のテスト方法について、詳しく説明します。

1 Kate O'Flaherty, Forbes, 「Marriott CEO Reveals New Details About Mega Breach」(2019 年 3 月 11 日)

2 Gartner, Inc., 『Market Guide for Network Traffic Analysis』(2019 年 2 月)

3 Jon Oltsik, CSO Online, 「Network traffic analysis tools must include these 6 capabilities」(2019 年 7 月 18 日)

重要な基準

ここでは、企業のお客様にとって最も重要な基準について説明します。

テストケース

IoT の可視化と脅威検出

IoT デバイスとは、モノのインターネット (IoT) を構成する多様なデバイスのことで、ネットワークに無線接続し、データ伝送機能を備える非標準的なコンピューティング・デバイスを意味します。IoT は、デスクトップ、ノート PC、スマートフォン、タブレットなどの標準的なデバイスだけでなく、従来のインターネット非対応物理デバイスや日用品にまでインターネット接続を広げます。IoT 技術が組み込まれたデバイスは、イントラネットとインターネットの両方で通信して対話でき、遠隔で監視および制御できます。そのため、これらのデバイスを通じて、悪意のある動作を行わせることも可能です。

テストでの考慮事項

IoT デバイスが(攻撃者の制御下にある)外部サーバーに接続してデータを宛先サーバーにアップロードしようとするときに、その活動を NTA ソリューションでどのように検出できるか。NTA ソリューションを展開する前から既にネットワーク内に侵害デバイスがあった場合に、問題を検出できるか。

ラテラル・ムーブメントの検出

Kerberos は、チケット・ベースのコンピュータ・ネットワーク認証プロトコルです。安全でないネットワークを介して通信する場合も、安全な方法でノードが相互に ID を証明できます。Kerberos 認証は、現在 Microsoft Windows で使用されているデフォルトの認証技術であり、Apple OS、FreeBSD、UNIX、Linux にも Kerberos の実装があります。Kerberos のユーザー ID 認証には、信用できる第三者による認証が必要です。

テストでの考慮事項

NTA ソリューションで、Kerberos のような認証プロトコルと、SMB や Microsoft Remote Desktop Protocol のようなアプリケーション・プロトコルを詳細に解析できるか。できないとしたら、認証情報の悪用やラテラル・ムーブメントのような脅威をそのソリューションでどのように検出できるか。

データ

アクティビティ・データはあらゆる NDR プラットフォームにとって血液のようなもので、送信元、送信先、送信者、送信元デバイスなど、ネットワーク上のトラフィックに関する情報を伝えます。現在のデータと過去のデータも含め、収集、使用、分析されるデータが広範かつ詳細であればあるほど、全体像や前後の状況を把握するのに役立ちます。

従来の NetFlow ベースのソリューションは、可視化の深度が限られており(ポートや IP アドレスなどのプロトコル情報のみ)、最新のデバイスや脅威を特定するコンテキストが不足しています。真の攻撃対象領域を把握し、最新の脅威を未然に阻止するには、ネットワーク・デバイスの状態や特定の生パケットに関するリアルタイムの真実のデータを入手できることが非常に重要です。

そこで、ネットワーク・トラフィックを詳細に可視化でき、メタデータだけでなくフルスタックのネットワーク・ログ、ネット・フロー、他のシステムのアラート、その他のデータ・サブセットも扱えるソリューションが必要になります。フルスタックのネットワーク・データを観測できれば、より広い範囲の脅威を見つけ出し、業務上の正当なアクティビティに紛れ込んでいる脅威も見つけやすくなります。

このツールには、IP アドレスだけでなく、デバイス、ユーザー、アプリケーション、組織など、多様な情報を可視化できる機能も必要です。この機能は、さまざまなエンティティ間の関係を解決し、垂直型通信と水平型通信において誤検知や検知漏れの少ない脅威検出を展開するのに役立ちます。

また、IoT のトラフィック、プロトコル、デバイスなどを監視する機能の必要性も高まっています。さまざまな種類の「モノ」をネットワークに接続する企業が増え、脅威対象領域が拡大するに伴い、重要性はさらに高まると予想されます。IoT セキュリティなどの特定のソリューションだけに限定せず、幅広いユースケースに対応するのが、最良の NDR プラットフォームです。

規制の厳しい業界などに属する一部の企業では、組織のデータ・プライバシーも重要な考慮事項になります。この問題には、NDR が顧客データをどこに保存し、どこで分析するかが関係してきます。一部のベンダーはデータをオンプレミスからベンダーのクラウドに移転させる措置を取っていますが、データをオンプレミスまたはプライベート・クラウドに保持する義務を負っている企業の場合、このような対応は規制違反となります。

ベンダーに確認すべき重要な質問

- どのデータ・ソースを NDR ソリューションへの入力に使用しますか？
- プラットフォームが提供するネットワーク可視化レベルはどのくらいですか？
- 何らかの理由でデータが顧客の環境の外部に持ち出されることはありますか？
- 組織におけるクラウド、モバイル、ハイブリッドのワークスペースの導入はどの程度進んでいますか？

データサイエンスとデータ分析

データサイエンスとデータ分析は、ネットワーク全体から集めたデータをもとに、有用なインサイトや情報を導き出す技術です。NDR ソリューションは、さまざまな科学的手法、プロセス、アルゴリズム、分析システムを利用して、構造化データおよび非構造化データからインサイトを抽出します。

その目的は、真の脅威に関する十分に詳細な情報を獲得して、自動対応を実施したり、セキュリティアナリストによる状況調査を行えるようにすることです。

データを個別のデータ要素として処理するだけでなく、データ全体に目を向け、ネットワーク内で誰がどのような状況でやり取りをしているかを把握することが大切です。つまり、どのデバイス、ユーザー、アプリケーションが対話し、どのように互いにやり取りしているのかを調べます。この相関付けと分析を自動化できる NDR ソリューションが理想です。

これが重要なのは、人間は IP アドレスで考えるわけではないからです。たとえば、「IP アドレス 10.1.2.3 で異常が発生している」という情報と、「マーケティング部門に所属する Windows PC ユーザーの Joe が、通常は財務部門の従業員が使用するアプリケーションにアクセスした」という情報では、どちらがセキュリティアナリストにとってより重要な意味を持つかを考えてみましょう。

もう 1 つ注目すべき点は、機械学習の専門用語で「特徴」(フィーチャー)と呼ばれる要素です。特徴とは、観測する現象の測定可能な個々の特性や性質のことです。

特徴は、シナリオにコンテキストを与えるのに役立ちます。たとえば、「デバイス A が大量のデータをクラウドにアップロードしている」というシナリオと、「デバイス A が Dropbox に大量のデータをアップロードしており、そのデータのソースは Python スクリプトである」というシナリオを比べてみましょう。どちらのアラートの方がセキュリティアナリストにとって有益かは一目瞭然です。

そのため、セキュリティに特化した特徴を多数抽出できるソリューションを選ぶことが大切です。その方が、誤検知の少ない高精度の脅威検出が可能になるからです。

ベンダーに確認すべき重要な質問

- この製品がどのように個々の観測を相関付け、フラグが付けられた動作やアクティビティに関するコンテキストを構築するかを説明してください。
- 脅威の検出に使用される、セキュリティに特化した機械学習の特徴の数と種類について説明してください。
- すべての異常に悪意があるわけではなく、すべての悪意ある動作が異常とは限らないという認識に基づき、フォローアップすべき真の脅威を見分けるようにシステムをトレーニングする方法について説明してください。

機械学習の活用

NDR ソリューションに関しては、どのような種類の機械学習を使用するかも重要な要素です。教師なし学習の場合は、人工知能(AI)アルゴリズムをトレーニングする際に、分類もラベル付けもされていない情報を使用します。これにより、学習した情報に基づいて動作する、ガイダンスを必要としないアルゴリズムを作り上げます。教師あり学習の場合は、入力データと望ましい出力データの両方をシステムに取り込み、分類用にラベル付けすることで、将来のデータ処理のための学習基盤を作ります。

テストケース

データ流出

DNS データ流出は、直接接続していない 2 台のコンピュータ間でデータを交換する手法です。データの交換は、中間 DNS サーバー上で DNS プロトコルを通じて行われます。流出フェーズでは、クライアントが外部 DNS サーバー・アドレスに対する DNS 解決要求を行います。攻撃者のネーム・サーバーは、A レコードで応答する代わりに、CNAME、MX、または TXT レコードで応答します。これにより、攻撃者と被害者の間で大量の非構造化データが送信可能になります。

テストでの考慮事項

NTA ソリューションは、このような脅威を発見するのに十分な詳細レベルで DNS を検査できるのか。それとも、攻撃者は大量にやり取りされる DNS トラフィックの盲点を悪用して検出を逃れることが可能か。

環境寄生型(現地調達型)攻撃の検出

内部脅威とは、組織内の人間に起因する、組織に対する悪意ある脅威のことで、従業員、元従業員、契約業者、業務関係者など、組織のセキュリティ対策、データ、コンピュータ・システムに関する内部情報を持つ人間が原因となります。

このテストケースでは、悪意のある内部関係者が、標的の内部にある通常システム管理ツールを悪用(つまり「現地調達」)してネットワークを列挙し、SMB 共有から機密データを収集します。

その後、攻撃者は盗んだデータをすべて、一般的なクラウド・サービス・プロバイダーのインフラストラクチャに置きます。

テストでの考慮事項

組織内部の人間による、正当な動作に見えて悪意のあるアクティビティを検出できるか。それはどのように実現されるか。

NDR ソリューションの中には、教師なし学習モデルのみを採用しているものがあります。そうしたソリューションは、まず数週間またはそれ以上かけてユーザーの環境を学習し、その後で、環境に何か変化があった場合に異常フラグを立てます。こうした表層的な機械学習アプローチは過剰な誤検知につながる可能性があり、場合によってはアルゴリズムの再トレーニングが必要になります。

たとえば、組織で新しいクラウドベースのデータ・バックアップ・ユーティリティを導入したとします。急に多くのユーザーが大量のデータをクラウドに送信するようになり、当初学習した動作と異なるため、NDR システムはこれを異常動作としてラベル付けします。

その結果、2つの問題が生じます。1つは、アナリストがこの異常な(しかし悪意のない)アクティビティの調査に無駄な時間を費やすこと、もう1つは、新しい動作パターンを学習させるために NDR システムの再トレーニングが必要になることです。後者の状況で、すべてのエンティティの動作をモデル化するのに再び数週間を要するシステムの場合は、それも運用コストに加味する必要があります。

教師なし学習と教師あり学習の両方を組み合わせたアプローチならば、何かが異常としてフラグが付けられた後の人間のアナリストの労力を軽減できます。

テストケース

マン・イン・ザ・ブラウザ攻撃の検出

電子メール、CRM、共同作業など、Web ブラウザを使用する業務は増え続けており、そのデータを傍受して操作できるプログラムや悪意のある攻撃者の存在は、企業にとって大きなリスクとなります。近年は、ブラウザの拡張機能を悪用する攻撃者が増えています。ブラウザの拡張機能は、高度なマルウェアに比べて簡単に作成でき、ソーシャル・エンジニアリングを通じて簡単にマシンにインストールでき、標的となるユーザーがブラウザでアクセスするすべてのものに自由にアクセスできるからです。

テストでの考慮事項

評価対象の NTA ソリューションに、悪意のある Chrome 拡張機能がデータを外部サーバーに無断アップロードするタイプのデータ窃盗を検出する機能があるか。

サポートされるユースケース

多くのセキュリティ・ツールは、お客様の環境で発生しやすいユースケースやシナリオに基づいて作られています。ソリューションでサポートできるユースケースが多ければ多いほど、そして、そのユースケースがセキュリティ業務に特化していればいるほど、ツールがセキュリティ・チームに提供できる価値が高まり、投資利益率 (ROI) をより短期間で実現できるようになります。

ソリューションでサポートされるユースケースの多様性には、2つの側面があります。1つは、組織の現在のセキュリティ・ニーズを支援すること。もう1つは、セキュリティ・プログラムの成熟に応じて、デジタル・フォレンジックや脅威ハンティングなどの機能の実行を支援することです。

優れた NDR ツールがサポートすべき最も重要なユースケースの例をいくつか示します。

既知の攻撃者 TTP の検出

これまで、大部分の脅威検出は侵害インジケータ (IoC) を利用して行われてきました。しかし、最近では攻撃者が巧妙になり、このインジケータが絶えず変化するので、より効果的に脅威を検出するために、攻撃者の戦術、技術、手順 (TTP) をモデル化する手法が採用されています。

たとえば、攻撃者が簡単に変更できる特定のドメインを探す代わりに、ドメインの背後にあるインフラストラクチャに注目します。それがどこに登録され、どこでホストされ、どの ASN (自律システム番号) をホスト・ネットワークに使用し、いつからドメインが存在するかなどです。

これらは攻撃者が簡単に変更できない事柄です。効果的な NDR ソリューションでは、こうした攻撃モデルをすぐに利用できます。さらに、お客様の組織に特化した TTP モデルをカスタマイズすることも、独自に作成することもできます。

脅威ハンティング

効果的な NDR プラットフォームは、脅威ハンティングを自動化する機能が必要です。セキュリティ・アナリストが求めているのは、セキュリティ・インシデントの状況把握に役立つ、既に関連付けられ、整理された情報です。セキュリティ・チームは、コンテキストに応じた不可欠なデータ、履歴のフォレンジック、AI ドリブン型の脅威ハンティング機能を利用することで、検出までの時間と修復までの時間の両方を短縮できます。

NDR プラットフォームだけでなく、ネットワーク・スイッチング・インフラストラクチャ自体にも脅威ハンティングを組み込めば、ディープ・パケット・インスペクションによるセキュリティ分析ソリューションを組織のネットワーク・ファブリックの一部として展開できます。

遡及的検出

新しい攻撃者の TTP が出現するたびに、組織はその TTP が過去に環境内で無意識のうちに発生していないかどうかを調査する必要があります。それには、過去にさかのぼって関連する動作を自動的に突き止め、攻撃のライフサイクル全体を可視化する機能が必要です。

たとえば、これまでネットワークに潜伏していて最近新たに見つかった攻撃タイプに関する情報が情報機関から発表されている場合があります。過去にさかのぼることで、その攻撃の兆候がネットワークになかったかを確認できます。

暗号化トラフィックの可視化

暗号化されるネットワーク・トラフィックが増加するにつれ、ポリシーやプライバシー上の理由から、復号化を積極的に行わない組織が増えていきます。この傾向を悪用し、ネットワーク脅威検出を回避する手段として暗号化トラフィックを使う攻撃者が出てきています。

暗号化トラフィック分析ソリューションを利用すると、通信を行っているアプリケーションや、回線を通過するトラフィックの性質などを特定できます。こうしたコンテキストは、非常に重要な意味を持ちます。

たとえば、暗号化されたファイルが Zoom 会議セッションで転送されるのは問題ないかもしれませんが、そのファイルが PowerShell スクリプトから Dropbox アカウントに転送されるとしたら、それは通常とは異なる動作であり、注意が必要です。

効果的な NDR ソリューションは、トラフィックの実際の内容を検査しなくても、暗号化トラフィックを分析して疑わしいものかどうかを判断する手段を提供します。さらに、このような分析を実行するためにエージェントをインストールする必要がない NDR ソリューションが理想です。

インシデント対応とフォレンジック

セキュリティ脅威が予防的なセキュリティ・ツールによって即座にブロックされず、インシデントに発展してから検出された場合は、人間のセキュリティ・スペシャリストが介入して対応する必要があります。

ネットワーク・トラフィックを分析すれば、誰が何をネットワーク上でアクティブになっているかを任意の時間間隔で正確に把握できます。NDR プラットフォームは、ネットワーク通信からエンドポイントのプロファイルを作成して、セキュリティ問題の解決に必要な情報を迅速に調査者に示せる必要があります。

ベンダーに確認すべき重要な質問

- NDR ソリューションでサポートされていて、すぐに利用できる具体的なユースケースの例を示してください。
- このソリューションは、組織に特化した自動脅威検出の作成と実行の手段を提供していますか？
- このソリューションは、ネットワーク可視化から、検出、調査、インシデント対応、デジタル・フォレンジックまでのセキュリティ運用ワークフローを、どのように効果的にサポートしていますか？

企業のバックグラウンド

ネットワーク脅威検出・対応のような先進的なソリューションにおいては、特定分野の詳細な知識と専門知識が何よりも大切です。ソリューション・ベンダーには、「セキュリティの DNA」と、ハイブリッド・ネットワークに関するデバイス・レベルの理解が求められます。ベンダーのバックグラウンドや、財務の安定性を考慮するのはもちろんですが、ネットワーク・トラフィック処理の中でも、ネットワーク・パフォーマンス管理といった側面より、ネットワーク層でのセキュリティ確保に関する経験を重視することを推奨します。この点は、製品のユーザー・エクスペリエンスやワークフローの実際の対象者に影響を与えることが多いからです。

ベンダーに確認すべき重要な質問

- このプラットフォームは、ネットワークのセキュリティ面に特化して設計されていますか？
- このプラットフォームは、今日のハイブリッド・ネットワークの要件に応えるようにスケーリングできますか？
- チーム（経営幹部や顧問も含む）は、セキュリティに関するどのような教育/経験/脅威研究の専門知識を持っていますか？
- 関連分野から派生した製品の場合、セキュリティ担当者にとって有効なワークフローにするために、どの程度の努力と脅威研究が行われましたか？

アリスタネットワークスジャパン合同会社

〒100-0004 東京都千代田区大手町 1-7-2 東京サンケイビル 27F
Tel: 03-3242-6401

西日本営業本部
〒530-0001 大阪市北区梅田 2-2 ヒルトンブラザウエストオフィスタワー 19F
Tel: 06-6133-5681

お問い合わせ先

Japan-sales@arista.com

Copyright © 2023 Arista Networks, Inc.

Arista のロゴ、および EOS は、Arista Networks の商標です。その他の製品名またはサービス名は、他社の商標またはサービス商標である可能性があります。

www.arista.com/jp

ARISTA

2022 年 4 月 25 日

セキュリティに重点を置いたネットワーク・トラフィック分析ソリューションのチェックリスト

セキュリティ脅威が予防的なセキュリティ・ツールによって即座にブロックされず、インシデントに発展してから検出された場合は、人間のセキュリティ・スペシャリストが介入して対応する必要があります。

データの特徴、特性、機能

詳細な可視化 - 評価対象のソリューションは、レイヤ 2 以上のフルスタックのネットワーク・トラフィックを可視化する はい いいえ

広範な可視化 - IP アドレスだけでなく、デバイス、ユーザー、アプリケーション、組織に関するデータを収集する はい いいえ

IoT、OT、クラウド・ネットワークのサポート - IoT、OT、クラウドのトラフィック、デバイス、プロトコルを監視できる はい いいえ

データ・サイエンスとデータ分析

データ・ポイントは、IP アドレスではなく、ネットワーク上のエンティティのコンテキストにおいて自動的に関連付けられ、分析される はい いいえ

誤検知の少ない高精度の脅威検出を可能にする、セキュリティに特化した「特徴」を多数提供する はい いいえ

異なる機械学習モデルの組み合わせ はい いいえ

ユースケース

攻撃をモデル化して既知の攻撃者 TTP を検出できる はい いいえ

攻撃の兆候の遡及的検出が可能である はい いいえ

暗号化トラフィックを復号化せずに可視化できる はい いいえ

導入企業側でユースケースと検出モデルをカスタマイズしたり、独自に作成したりできる はい いいえ

インシデント対応、フォレンジック、脅威ハンティングが可能である はい いいえ

展開と拡張性

大量のセンサーを必要とせずに、広範囲にネットワークをカバーできる はい いいえ

物理センサーにするか仮想センサーにするかを必要に応じて選択できる はい いいえ

ソリューションは、他のセキュリティ・ツールと適切に連携するプラットフォームである はい いいえ

分析のどの部分にもエンドポイント・ソフトウェア・エージェントは不要である はい いいえ

ハイブリッド・ネットワークのセキュリティ・ニーズに合わせてソリューションをスケーリングできる はい いいえ

企業のバックグラウンド

プラットフォームはセキュリティ分析に特化している はい いいえ

ソリューション・プロバイダーは、セキュリティに関する豊富な経験と専門知識を持っている はい いいえ

ソリューション・プロバイダーは、ネットワーク層でセキュリティを構築できる はい いいえ

用語集

Advanced Persistent Threat (APT、高度で持続的な脅威): NIST は APT のことを、複数の攻撃ベクトル(サイバー、物理、欺瞞など)を使用して目的達成の機会を生み出せる高度な専門知識と多大なリソースを持つ攻撃者と定義しています。

通常、その目的は、情報流出や、ミッション、プログラム、または組織の重要な側面の弱体化や阻害、あるいは将来の目的達成の準備として、標的となる組織の情報技術インフラストラクチャ内に足がかりを確立して広げることにあります。

APT には次の特徴があります。(i) 長期間にわたって繰り返し目的を追求し、(ii) 防御者の対抗策に適応し、(iii) 目的を果たすために必要なインタラクション・レベルの維持を執拗に試みます。

水平トラフィック移動(ラテラル・ムーブメント): 水平移動(ラテラル・ムーブメント)は、サイバー犯罪者が流出させるデータまたは資産を探索するためにネットワーク内を系統的に移動する手法です。これは目的を達成するための手段であり、機密データを特定し、アクセスし、流出させるための技法です。

攻撃者は、多様なツールと方法を使用して高い権限とアクセス権を得ると、ネットワーク内を横移動(デバイス間やアプリ間を横展開)し、システムをマッピングしてターゲットを特定し、最終的に組織の重要資産に到達します。たとえば、攻撃者が管理者権限を入手した場合、悪意のあるラテラル・ムーブメントのアクティビティは、それを見分けるツールがなかったり、大量のアラートに忙殺されたりしているセキュリティ担当者には「正常」なネットワーク・トラフィックに見えるため、検出が極めて困難になります。

内部脅威: 内部脅威は、組織内部に起因する組織のセキュリティ・リスクです。これは、組織のデータとコンピュータ・システムにアクセスできる(またはアクセスできた)現従業員、元従業員、契約業者、その他の業務関係者が原因で発生する可能性があります。内部脅威は組織内部から発生し、故意の場合とそうでない場合があるため、あらゆる攻撃タイプの中でも特に被害が大きく、検出が困難なものの1つです。

ネットワーク脅威検出・対応(NDR): ネットワーク脅威検出・対応は、悪意のあるネットワーク・アクティビティの検出と防止、根本原因を特定するための調査とフォレンジックの実行、対応とリスク低減の戦略を行うために組織が使用するセキュリティ・ソリューションのカテゴリです。NDR ソリューションは、より深いレベルでネットワーク・データを解析し、誤検知と検知漏れが多く発生しやすい教師なし学習(異常検出)に依存せずに、異なる機械学習アプローチの組み合わせを使用します。

これらのプラットフォームは、状況認識と検出から、インシデント対応、脅威ハンティング、デジタル・フォレンジックまで、幅広いユースケースをサポートします。

インサイダー攻撃、認証情報の悪用、ラテラル・ムーブメント、データ流出など、マルウェア以外の脅威に対する保護機能を備えた NDR ソリューションは、実際にネットワーク上にあるもの、および発生するすべてのアクティビティに関する可視化を高めます。これにより、セキュリティ・チームは、疑わしいネットワーク・アクティビティを迅速に特定して阻止することができるため、影響を最小限に抑えることができます。

垂直トラフィック移動: 垂直移動では、トラフィックはインターネット空間へのネットワークを出入りします。つまり、エッジ・ファイアウォールやルーターを出入りします。

脅威ハンティング: 脅威ハンティングは、経験豊富なサイバーセキュリティ・アナリストが、手動または機械ベースの技術を予防的に使用して、現在展開されている自動検出方式では検出できなかったインシデントまたは脅威を特定するプロセスです。

脅威ハンティングを成功させるには、ツールセットを適切に活用して特に危険な脅威を発見する方法をアナリストが知っている必要があります。また、ログ、メタデータ、パケット・キャプチャ(PCAP)データからなる大量のデータを扱うために、さまざまな種類のマルウェア、エクスプロイト、ネットワーク・プロトコルに関する十分な知識も必要です。