SOPHOS
Cybersecurity delivered.

脅威ハンティングを始めるにあたり

掴みどころのないサイバー脅威を検索し、無力化するための準備に関する実践的なガイダンス

サイバー攻撃は進化しています。攻撃者は、攻撃を簡単に実行するために、巧妙で高度な回避的手法にますます注目するようになっています。そのため、悪意のあるアクティビティを探して無力化する対策が、高度な脅威との戦いにおいて重要になってきました。しかし、それは容易なことではありません。

このレポートでは、脅威ハンティングを開始するためのガイダンスと、最新のサイバー脅威に常に先回りして対応し、潜在的な攻撃への迅速な対応を支援するために、セキュリティチームが活用しているツールとフレームワークの概要を紹介します。また、IT 管理者が脅威ハンティングに備える際に行うべき 5つのステップについても説明します。

ソフォス ホワイトペーパー2022年 8月

2022年のサイバー脅威の現状

攻撃の量、複雑さ、影響の増大

組織が直面するサイバーセキュリティの問題は増加する一方です。過去 1年間で、57% の組織がサイバー攻撃の量の増加を経験し、59% が攻撃の複雑さが増し、53% が攻撃の影響が増大したと述べました。そして、約 4分の 3 (72%) が、これらの領域のうち少なくとも 1 つで増加を実感しています。

2021年 3月に明らかになった SolarWinds 事件のように、サプライチェーンへの攻撃が増加する傾向にあります。攻撃者は、複雑なネットワークをリモートで管理するために使用される同社の Orion ソリューションのソースコードに修正した命令を挿入していました。このバックドアにより、攻撃者は複数の政府機関を含む SolarWinds 社の顧客のネットワークにアクセスすることができるようになりました。

すべての組織にとって真の脅威はランサムウェア

ランサムウェア攻撃を受けた組織の割合は、2020 年の 37% から増加し、2021 年は 66% でした。これは 1 年間で 78% の増加であり、攻撃者が攻撃をさらに大規模に実行する能力がかなり向上していることを示しています。

サイバー攻撃における正当なツールの使用の増加

攻撃者は、正当な市販のソフトウェアや無料のオープンソースツールの違法版または海賊版をますます活用しています。通常、これらのツールは、セキュリティを向上させるためにサイバー攻撃をシミュレートするように設計されていますが、犯罪者が悪用してそれとは逆のことをする可能性があります。

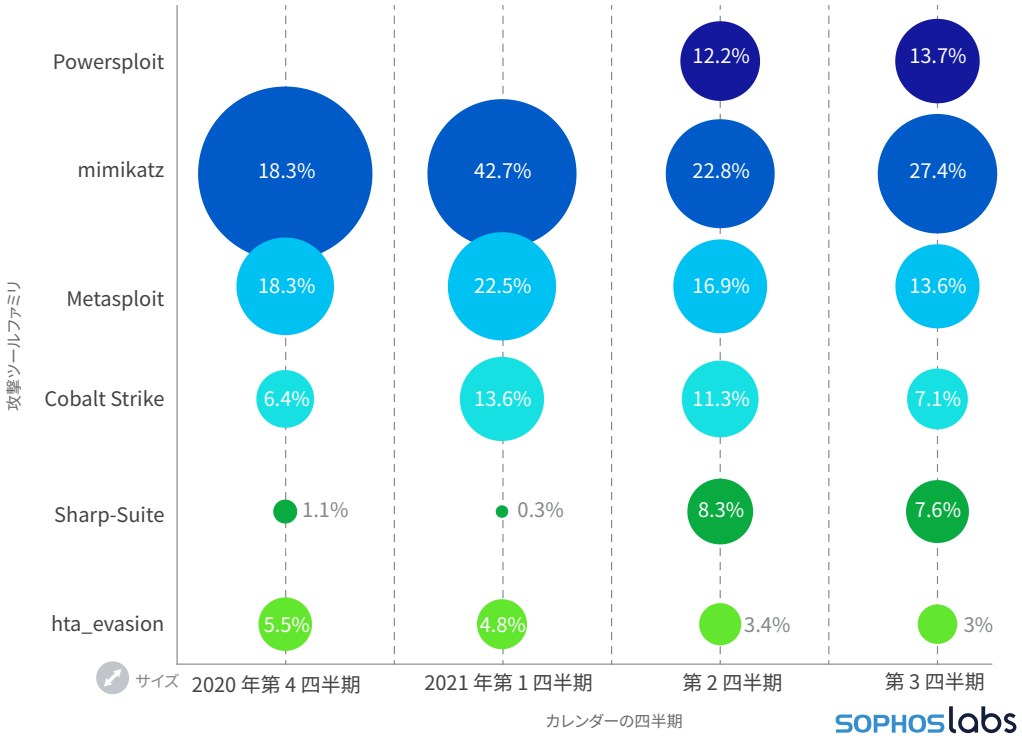
Mimikatz（ペネトレーションテスト担当者やマルウェア作者が使用）のようなツールは、厳密には商用製品ではありませんが、広く使用されており、ソフォスが過去 1年間に調査したほぼすべてのハンズオンキーボード攻撃で使用されています。

また、特に目立ったのは（2020年にソースコードが流出したおかげで）、Cobalt Strike（攻撃者のシミュレーションソフトウェア）の海賊版で、ランサムウェア攻撃に使われていただけでなく、他のマルウェアの初期ペイロードとしても使用されていたものでした。

[1]ランサムウェアの現状 2022年版 - ソフォス
[2]ランサムウェアの現状 2022年版 - ソフォス

上位の攻撃ツールの普及率

2020-2021 年で最も頻繁に発生した攻撃ツール、マシン単位



2022年版ソフォス脅威レポート

Windows マシンに有能なバックドアを提供する Cobalt Strike の「Beacons」機能は、このソフトウェアがサイバー犯罪者にとって好ましいツールになったことを意味します。そういう訳で、過去 1年間で見てきたランサムウェア事例のほとんどは、Cobalt Strike Beacon を使用したものになっています。

サイバー脅威の現状については、最新のソフォス脅威レポートをご覧ください。

プロアクティブなサイバーセキュリティ対策は必須

サプライチェーン攻撃、ソフトウェアエクスプロイトや正当なツールを使用した悪用。ここでの共通しているテーマは、これらのアプローチの性質です。これらのアプローチは人間主導であり、非常にターゲットを絞って計算され、回避的で、従来の手段では検出できません。

組織は、犯罪者の一歩先を行くために、よりプロアクティブなサイバーセキュリティのアプローチに移行する必要があります。人間の敵に対応するには、人間主導のアプローチが必要です。

そこで、脅威ハンティングの登場です。

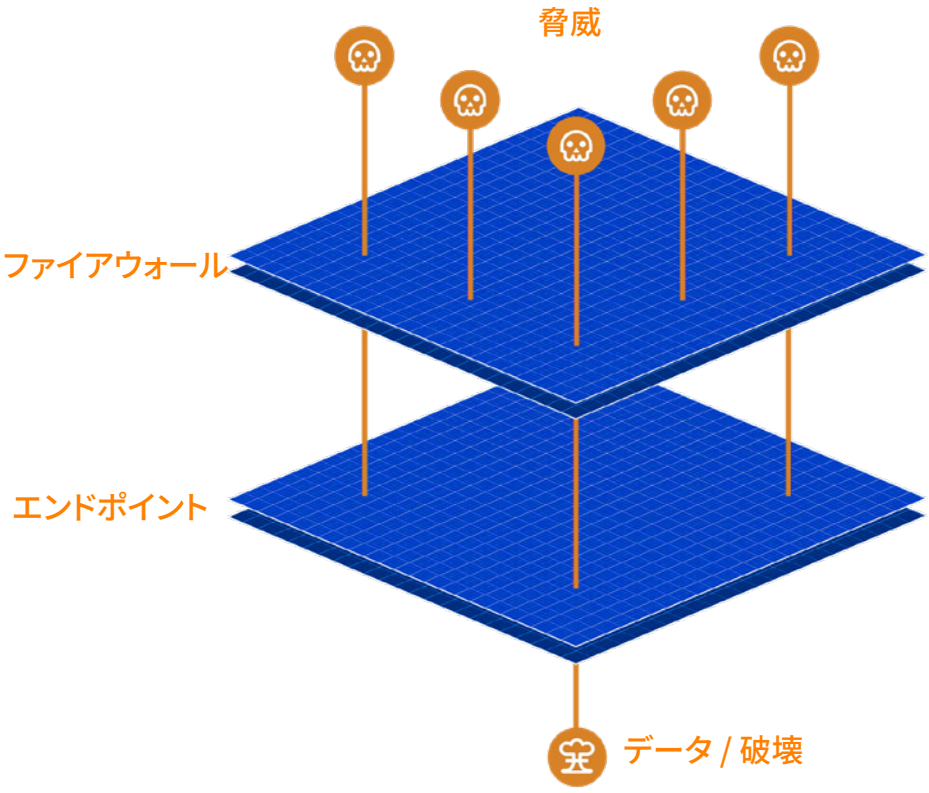
脅威ハンティングとは?

脅威ハンティングとは、エンドポイントやネットワークのテレメトリを検索して、悪意のあるアクティビティを特定するための反復的かつプロアクティブなプロセスであり、攻撃者がすでに防御を回避していることを前提に行われるものです。今日の進化するサイバー脅威を探して無力化するための効果的な方法であり続けるために、常に対策を適応させるよう、繰り返し分類していきます。

脅威ハンティング中に、チームは脅威アクターが使用するツール、テクニック、および手順 (TTP) を分析して、攻撃の段階を判断し、情報を構築します。これが確立されたら、必要に応じて脅威を無力化するための適切な措置を実行します。

なぜ脅威ハンティングをする必要があるのですか。

その理由は複数あるのですが、全体的な理由の 1つとしては、「無数の主張に反して、テクノロジーだけでは脅威を 100% を阻止することはできない」という真実からです。多層型の防御を講じているにもかかわらず、一部の脅威は依然として IT 資産に侵入し、危険にさらしています。



すでに述べたように、現代の脅威アクターは、昨年の自動化された大規模な攻撃ではなく、文字通り「ハンズオンキーボード」による適応型および回避的なアプローチにますます注目しています。

これは、攻撃を制御したり、駆逐する人間の攻撃者の数が大幅に増加したことを報告している脅威対応チームの調査結果を反映しています。つまり、セキュリティチームは、侵害がすでに発生していると考え方を取り入れながら、敵の一歩先を行くために未知の脅威を捜し続ける必要があることを意味しています。

脅威ハンティングの考え方

経験豊富な脅威ハンターは、潜在的な脅威が攻撃チェーン内のどこに存在するにか関わらず、すでに防御を回避していると一般的に想定します。脅威ハンターがこのような考え方をする理由は、2つのことをしなければならないからです。

脅威アクターの滞留時間を制限

このような考え方を採用することで、セキュリティチームは脅威アクターの滞留時間を制限することができます。ハッカーがネットワーク内にいる時間が長いほど、悪意のあるアクティビティを実行する時間が長くなります。そのため、攻撃者のネットワーク内の滞在時間が短いほど、被害は少なくなります。セキュリティチームは、防御をすでに回避したと想定することで、影響を受ける前に脅威を探すことを余儀なくされています。

検出 への時間を短縮

この考え方を採用することで、チームは検出までの平均時間を短縮することもできます。多層防御を施しており、回避した脅威が攻撃チェーンに沿って防御をさらにトリガーするかもしれません。問題は、この時点では手遅れだということです。脅威がすでに拡大しすぎているため、被害が発生しています。脅威を探すことで、セキュリティの弱点を特定し、後に対処できるようになります。これにより、将来的に同様の、または類似した脅威を検出する時間が短縮できる可能性があります。

脅威ハンティングは誰が行いますか?

脅威ハンターのプロファイル

誰が脅威ハンティングを行うかについて説明する前に、脅威ハンターの役割を理解することが先決です。脅威ハンティングの操作は非常に複雑です。この分野の担当者は、特定のニッチなスキルが必要です。とはいえ、脅威ハンターに求められる典型的な特徴は次の通りです。

- **創造的で好奇心旺盛** – 脅威を探すことは、針穴に糸を通すような作業と似ています。脅威ハンターは、脅威を発見するためにさまざまな方法を駆使して、何日もかけて脅威を探すことがよくあります。
- **サイバーセキュリティの経験** – 脅威ハンティングはサイバーセキュリティの中でも最も高度な業務の 1つです。そのため、これまでの現場での経験や基礎知識は必須となります。
- **脅威の状況に関する知識** – 未知の脅威を探し出し、無力化するためには、最新の脅威の傾向を理解することが不可欠です。
- **攻撃側の思考** – ハッカーのように考える思考力が、今日の人間主導のアプローチに対抗するには重要となります。
- **テクニカルライティング能力** – 脅威ハンターは、調査プロセスの一環として、すべての発見事項を記録する必要があります。そのため、このような複雑な情報を伝える能力は、ハンティングを最後まで追跡する上で非常に重要です。
- **OS とネットワークに関する知識** – 両方の高度な実務知識が不可欠です。
- **コーディング / スクリプトの経験** – 脅威ハンターがプログラムの構築、タスクの自動化、ログの解析、データ分析タスクの実行と調査を支援および進行する際に必要です。

残念ながら、このような稀な能力を持ち合わせることは、IT 分野で顕著なスキル不足になっており、IT 管理者の 54% は、すべてのツールを自由に使用できたとしても、サイバー攻撃は高度過ぎて IT チームが単独で対処できないと考えています。このことから、役割を果たせる場合は、2つの異なるチームのうちのどちらかが、脅威ハンティングを実行していくことが一般的です。

社内セキュリティ オペレーション センター (SOC)

組織が自ら脅威ハンティングを行うことを選択した場合、SOC 内で雇用されることがあります。SOC は、サイバー脅威の監視、検出、調査、対応に焦点を当てた社内の一元管理機能であり、親組織の包括的なセキュリティ体制を強化します。これは、サイバーセキュリティに関する組織内の相談窓口となるチームです。

第三者機関のセキュリティ オペレーション プロバイダ

多くの組織では、セキュリティ運用を第三者機関のプロバイダにアウトソーシングする傾向がますます高まってします。これは、社内での能力が不足していること (IT チームは昨年、サイバーセキュリティの作業量が 69% 増加)、スキルが不足していること、またはこの24時間年中無休のサポートが必要な重要な業務を外部の専門家に任せることが起因している可能性があります。

MDR (Managed Detection and Response) プロバイダ

フルマネージド型サービスとして提供される MDR は、24時間年中無休で潜伏している脅威を探すセキュリティアナリストの専門チームで組織を支援します。実際、ESG Research によると、「51% が MDR (マネージド検出と応答) サービスプロバイダを利用して、脅威の検出と対応のためのテレメトリデータの統合を支援している」とのことです。

MDR プロバイダーには、社内のみのセキュリティ運用プログラムとは異なるさまざまな利点を備えています。その中でも最も大きな利点は、多くの場合、経験だと言えます。

Sophos MDR チームは、数千時間にもおよぶ経験を持ち、攻撃者が仕掛けるあらゆるものを見て、対処してきています。また、ある組織に対する攻撃から学びを得て、それをすべての顧客に適用しています。もう 1つの利点は規模です。Sophos MDR チームは、3つのグローバルチームによって 24時間年中無休のサポートを提供できます。

マネージド セキュリティ サービス プロバイダ (MSSP)

MSSP は、組織の IT セキュリティ運用の一部またはすべてを管理するので、社内チームは日常業務により集中することができます。MSSP は、マネージドサービスの一部として脅威ハンティング機能を提供します。これには、前述の MDR サービスが含まれる場合があります。

脅威ハンティングイネーブラー

Endpoint/Extended Detection and Response (EDR/XDR)

脅威ハンターが潜在的に悪意のあるアクティビティを特定し、調査するには、情報と調査ツールが必要です。 EDR および XDR を導入してください。これらにより、ハンターは疑わしい検出をすばやく確認し、それらを徹底的に調査することができます。

名前が示すように、EDR はエンドポイントソリューションからの情報を提供します。一方、XDR は、ファイアウォール、モバイル、メール 、クラウド セキュリティ ソリューションなど、幅広い IT 環境からの信号を統合します。攻撃者があるゆる攻撃の機会を悪用することを考えると、信号網を広く張り巡らせれば張り巡らせるほど、攻撃を早期発見できるようになります。

EDR/XDR ソリューションの実用上の最大の課題の1つはノイズです。脅威ハンターは非常に多くの信号を受け取るため、木を見て森を見ずになる場合があります。そのため、EDR/XDR ソリューションと強力なエンドポイント保護を組み合わせることが不可欠です。これにより、より多くの脅威を未然に防ぎ、防御者はより少ない、かつより正確な検出に集中することができます。

脅威の検出と対応の構造

脅威ハンティングは、脅威検出および対応という、より広範な業務の一部です。ソフォスでは、脅威の検出と対応のフレームワークをハンティングに適用しています。これは、5つのコアコンポーネントで構成されています。

1.予防

堅牢で適切に設定された防御テクノロジー (エンドポイント保護ソリューションなど) を導入することで、攻撃者がネットワークに侵入することを防ぎます。さらに重要なことは、日ごと、あるいは 1時間ごとに発生するセキュリティの警告数も減少するということです。警告の数が減ることで、セキュリティチームは重要な信号 (この場合、回避的な人間主導の攻撃者) をより的確にとらえ、集中的に対処できるようになります。

2.セキュリティイベント、警告、および検出の収集

データは、脅威ハンティングと脅威解析の原動力となる燃料です。信号の適切な種類、量、質なしでは、セキュリティ運用チームは潜在的な攻撃指標を正確に特定することは困難です。しかし、コンテキストのないデータは、アナリストが納得のいく判断をしづらくします。信号に関連する意味のあるメタデータがないと、アナリストはその信号が悪意のあるものか無害なものかを判断することが困難になります。

3.重要な信号の優先順位付け

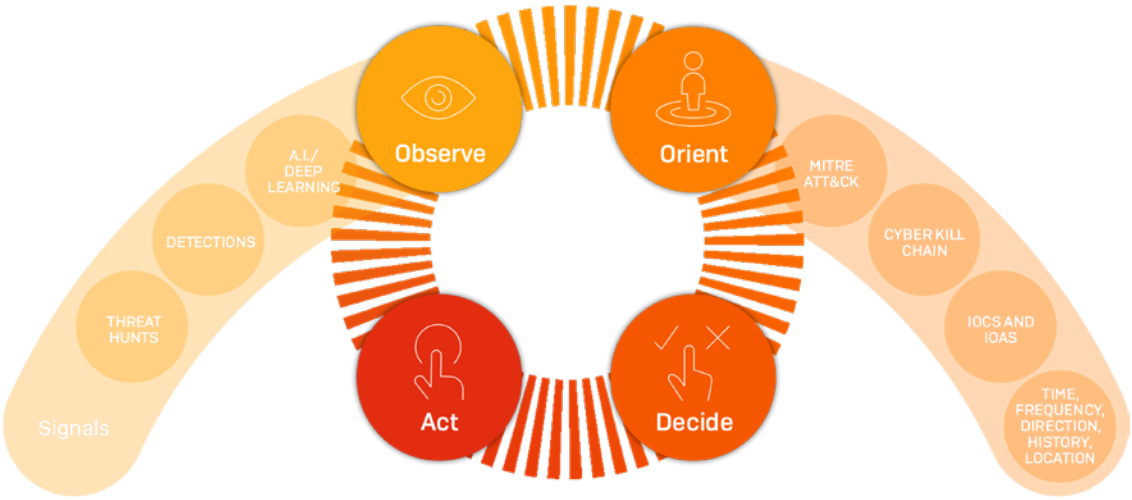
データに圧倒されたり、詳細な調査が必要な項目を見落とさないようにするためには、重要な警告をピンポイントで特定する必要があります。これは見た目以上に難しいことです。イベント製作者のみが提供できるコンテキストと自動化された人工知能を組み合わせることで、S/N 比を向上させることができます。自動化しても、それは簡単な作業ではありません。

4.調査

重要なシグナルを特定したら、業界のフレームワークやモデルを照らして発見したことを洞察、測定し、悪意のある動作または無害な動作かを確信するしきい値を構築します。

OODA 調査のフレームワーク

経験豊富なセキュリティアナリストは、多くの場合、調査の指針としてフレームワークを活用します。たとえば、Sophos MDR チームは、OODA ループと呼ばれる調査方法を使用しています。 これにより、前述したサイクルを行い、すべての調査結果がテスト・証明されていることを確認できます。



OODA ループは、軍事的な概念であり、ソフォスのチームが推論サイクルを経て、イベントとその周囲の行動を完全に理解できるようにします。その後、この知識をもとに、人間の意志決定と直観を活用して、悪意のあるアクティビティがお客様の環境内に存在するかどうかを判断し、それに基づいて、その行動方法を決定できます。

OODA フレームワークを適用する場合、ソフォスのセキュリティアナリストは、多くの場合、次の手順を実行します。

- **観察 - この検出でどんな状況がわかるか?**
  - 検出に関連する外部、および内部の潜在的なつながりの観察
  - 検出が行われている場所と、エンドユーザーが検出に関連付けられているかどうかを確認
- **仮説構築 - この検出で何を理解しているか?**
  - 証拠に基づくデータを収集
  - この攻撃や脅威アクターへの共通もしくは固有の TTP を理解する。TTP を特定するために使用されるこのようなリソースの 1つに、MITRE ATT&CKフレームワークがあります。これについては、レポートの広範で詳しく説明します。
  - 攻撃の指標(IOA)および感染の痕跡(IOC)に関するインテリジェンスを収集
- **意志決定 - この検出は悪意があるか、疑わしいか、または無害なものか?対処が必要か?**
- **行動 – これまでの手順を踏まえて、何をするのか?**
  - **緩和 - 無力化 - 再ループ - 改善。**

5.アクション

今から話すことは大切なことです。脅威に対応していると判断したら、2つのことを行う必要があり、このどちらも同じぐらいに重要です。

1つ目は、目先の問題を軽減すること、2つ目は、攻撃の症状に対処しているだけであり、根本的な原因を突き止めて無力化する必要があることを覚えておくことです。1つ目の作業は、2つ目の作業を妨げることなく実行する必要があります。

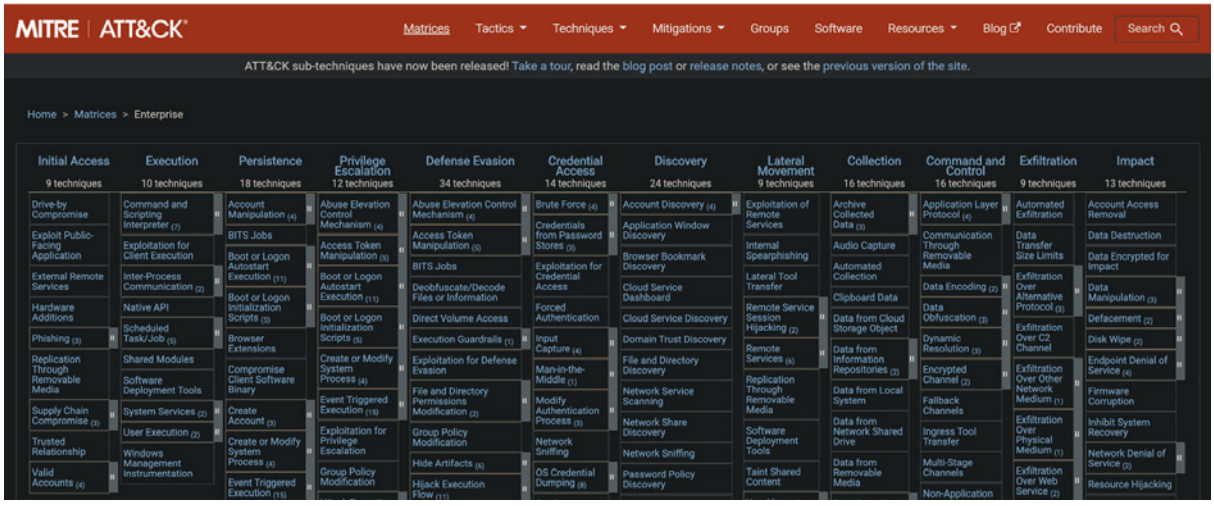
マシンを隔離したり、ネットワークから切り離すだけで済む場合もあれば、セキュリティチームがネットワークの奥深くまで入り込み、攻撃者の痕跡を探し出す必要がある場合もあります。

たとえば、システムからマルウェアを正常にブロックして削除し、警告が表示されなくなったからといって、攻撃者が環境から排除されたわけではありません。

何千もの攻撃を見てきたプロの脅威ハンターは、いつ、どこを深く調べるべきかが分かります。オペレーターは攻撃者がネットワーク上で実行していること、してきたこと、これから実行を計画する可能性のあるものを探し、それらも無力化します。

脅威の分類：MITRE ATT&CK フレームワーク

脅威ハンターがよく使用するリソースは、MITRE ATT&CK フレームワークです。サイバーセキュリティに時間を費やしたことがあれば、少なくとも聞いたことがあるのでしょう。MITRE は、多くのフレームワークの中で、実際の調査に基づいた攻撃者の TTP の世界的にアクセス可能な知識ベースであり、特定の脅威モデルや方法論を開発するための基盤として利用されています。これにより、脅威ハンターは攻撃者の行動を過去に特定された膨大な数の TTP にマッピングでき、ハンターはライフサイクルのどの段階で進行中の攻撃が発生しているかを確認することができます。OODA フレームワークの「仮説構築」段階では、このことが重要です。



MITRE ATT&CK フレームワークの詳細については、ここをクリックしてください。

脅威ハンティングの方法

このセクションでは、一般的に採用されている脅威ハンティングの方法について説明します。ソフォス では、2つの異なる方法でハンティングを開始することがしばしばあります。

リード主導型脅威ハンティング

ソフォスでは、さらなる調査が必要な検出は、あらゆる状況にビジネスコンテキストと人間の推論を適用できる人間の脅威アナリストがレビューします。振る舞いを観察し、それまでに確立されたビジネスコンテキストを検討し、仮説を立て、それに基づいて行動します。仮説は、潜在的なインシデントに積極的に関与することかもしれないし、またはさらなる調査作業を実行して、目の前の問題について知識をより強化することかもしれません。

ループを完了させるには、アナリストはその仮説と検証の結果を確認するために待機して、レビューします。さらに調査が必要な場合は、結論が出るまでこのサイクルを繰り返すことができます。イベントがアクティブなインシデントに発展した場合、アナリストは脅威を積極的に対処するためにフルレスポンスモードに切り替わります。

リードレス (手掛かりなし) の脅威ハンティング

リード主導型ハンティングでは、対象の「信号」を検出・生成するためにセンサーの 1つが必要ですが、リードレスハンティングでは、より本質的なものとなります。未だに AI アルゴリズムを使用して、大量のデータを処理しているかもしれませんが、リードレス脅威ハンティングでは、ほぼ常に人間の脅威アナリストが管理しています。

最初の体系的な信号に依存して、調査が必要なものを知らせるのではなく、顧客の環境全体に積極的にクエリを実行します。このことは、以下に限定されるわけではありませんが、次の理由が挙げられます。

- 同じ業種の顧客が特定の方法で標的にされていおり、同じ脅威アクターがソフォスの他の顧客を攻撃しようとしていないことを確認するために、デューデリジェンスの実行を希望
- SophosLabs は、同じ業種または類似のプロパティを持つ顧客を標的として重大な攻撃について MDR チームに通知済
- セキュリティ環境で重大なイベントが発生し、当社のお客様が影響を受けていないか確認の希望

導入事例：銀行を狙う歴史的なトロイの木馬を発掘したランサムウェアハント

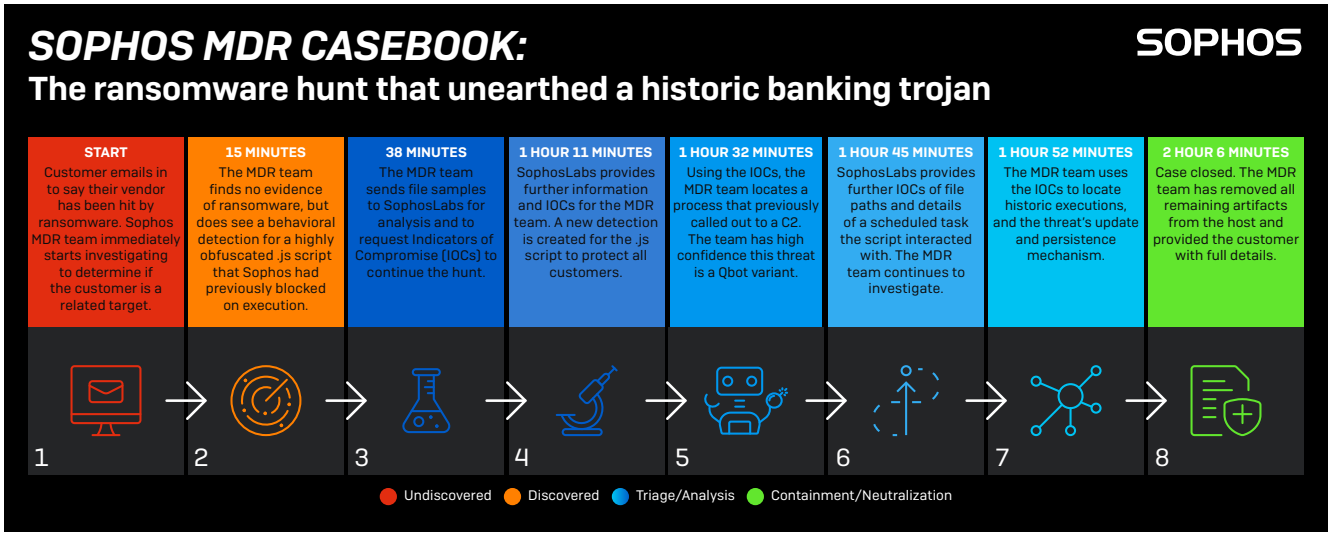
ここまで、脅威ハンティングの複雑さについて説明しました。次に、脅威ハンティングの動作を説明していきます。Sophos MDR が調査したこのケースは、脅威ハントが予期しない事態をどのように発見するかを示す良い例です。このケースでは、お客様は、取引先のベンダーがランサムウェアに感染したので、自分たちも感染しているのではないかと心配していました。

Sophos MDR チームは、SophosLabs の専門家と協力して、すぐに調査を開始しました。お客様その後すぐにランサムウェアの証拠がないことに気づきました。この時点で、一部のチームはケースをクローズして、他の作業に移ったかもしれません。しかし、Sophos MDR チームは引き続き調査を行い、歴史的なバンキング型トロイの木馬を発見しました。

お客様は、ランサムウェアの被害に遭わなかったこと、そして歴史的なバンキングマルウェアが完全に削除されていること知って安心しました。この結果は、専門家の介入なしでは実現できませんでした。

この話からわかるように、ランサムウェアはしばしば念頭に置かれる脅威ですが、影に隠れて攻撃をするパターンにも警戒が不可欠です。

2時間 6分以内で、すべてのインシデントが調査され、クリーンアップされました。



このケースについての詳細は、こちらの記事をお読みください。

脅威ハンティングの準備 - 成功を支援する 5つのステップ

これで、脅威ハンティングに関連するあらゆることを十分に把握できるようになります。ただし、作業を開始する前に、効果的に実行するための最適な設備が組織に整っていることを確認することが不可欠です。

1.現在のサイバーセキュリティ運用の成熟度を把握

潜在的な攻撃者を理解する前に、現在のサイバーセキュリティ運用の状態を理解する必要があります。プロセスをサイバーセキュリティの成熟度モデル (CMMC など) にマッピングすることは、脅威ハンティングを開始するための設備が整っている (または整っていない) ことを確認する最適な方法です。また、セキュリティポスチャを監査して、脅威の影響を受けやすいかどうかを判断することもお勧めします。

2.脅威ハンティングをどのように対処したいか決定

サイバー成熟度を確立したら、脅威ハンティングを社内で行うか、完全にアウトソーシングするか、またはその両方を組み合わせて行うかを決定できます。

3.テクノロジーのギャップを特定

既存のツールを見直し、効果的な脅威ハンティングを実行するために必要なものを特定します。防御テクノロジーはどの程度効果的ですか。EDR/XDR によってもたらされる脅威ハンティング機能を備えている、またはサポートしていますか。

4.スキルのギャップを特定

脅威ハンティングは複雑で、専門的なスキルが必要です。社内での経験がない場合は、トレーニングコースを探して、必要なスキルを身に付けることができます。また、チームを補完するために、サードパーティのプロバイダと協働することもご検討ください。

5.インシデント対応計画の策定と実施

脅威ハンティングを開始する前に、あらゆる対応を測定し制御するために、本格的なインシデント対応を実施することが不可欠です。 すべての主要な関係者がすぐに実行できる、十分な認識を持ち、準備の行き届いた対応計画を立てることで、組織への攻撃の影響を劇的に減らすことができます。

優れたインシデント対応計画は、準備、検出、報告、トリアージと分析、封じ込めと無力化、およびインシデント後のアクティビティに関するプロトコルの概要を説明する必要があります。効果的なインシデント対応計画を構築するためのヒントについては、インシデント対応ガイドを参照してください。

脅威ハンティングの準備と実施に関するより実践的なガイダンスについては、Sophos Threat Hunting Academy をご覧ください。

ソフォスが提供する支援

先ほど述べたように、効果的な脅威ハンティングは非常に複雑であり、広範な人間の専門知識とを組み合わせた次世代テクノロジーが必要です。幸い、ソフォスはサイバーセキュリティ成熟度に関係なく、脅威ハンティングの目的をサポートできます。

脅威のネットワーク侵害を防止 - Sophos Intercept X Endpoint

脅威ハンターは、セキュリティ警告が少ない場合のみ、その役割を効率的に実行できます。これを実現する一つの方法は、業界最高レベルの防御テクノロジーを導入することです。これにより、防御側は、より少ない、かつ正確な検出に注力でき、その後の調査と対応プロセスを合理化することができます。Sophos Intercept X Endpoint を導入ください。

Sophos Intercept X は、業界をリードするエンドポイントセキュリティソリューションで、攻撃対象領域を減らして、攻撃の実行を防止します。エクスプロイト対策、ランサムウェア対策、ディープラーニング AI、制御テクノロジーを組み合わせることで、システムに影響を与える前に脅威を阻止します。Intercept X は、1つの主要機能に依存することなく、エンドポイント保護への包括的な多層防御のアプローチを使用しています。

Sophos Intercept X エンドポイント保護の機能は、脅威の 99.98% をブロックします（AV-Test平均スコア 2021年1月～11月）。防御側は、人間の介入を必要とする疑わしい信号により注力することができます。

Intercept X Endpoint の詳細または無償版については、こちらをご確認ください。

脅威の監視を自身で実施 – Sophos XDR

Sophos XDR は、SOC 専任チームのセキュリティアナリストや IT 管理者向けに設計されており、エンドポイント、サーバー、ファイアウォール、クラウドワークロード、メール、モバイルなどにおけるインシデントの検出、調査、および対応を利用できます。

事前に作成され、カスタマイズ可能なテンプレートをライブラリから選択して、重要な情報をすぐに入手。テンプレートはさまざまな脅威ハンティングや IT 運用のシナリオに対応しています。また、独自のテンプレートを作成することもできます。デバイスのライブデータ、最大 90日間のオンディスクデータ、Sophos Data Lake のクラウドリポジトリに保存されている 30日間のデータ、さらに疑わしい項目の自動生成リストにアクセスできるので、即座に調査を開始できます。

独自の脅威ハントを実行するために Sophos XDR をお試しになりたい場合は、ソフォスは高度な脅威ハンティングとセキュリティ運用の予防策に必要なツールを用意しています。製品版トライアルを開始する (Sophos Central のアカウントをお持ちの場合) か、XDR が含まれる Sophos Intercept X のトライアルをご利用ください。

フルマネージドサービスとして、またはチームを補完するための脅威ハンティング – Sophos MDR

Sophos MDR は、受賞歴を誇る多面的、包括的な MDR ソリューションで、ソフォスのセキュリティアナリストチームの専門知識とスキル、およびネットワーク環境とクラウド環境に対応する豊富な機能を備えています。ソフォスは、膨大な機能をお客様のセキュリティ運用に追加することで、セキュリティ運用を効果的に拡張します。

脅威ハンターと対応の専門家である Sophos MDR チームは、次のことを行います。

- 潜在的な脅威とインシデントをプロアクティブに追跡し、検証
- 利用可能なすべての情報を使用し、脅威の範囲や重大度を判定
- 有効な脅威に対して適切なビジネスコンテキストを適用
- 脅威をリモートから阻止、封じ込め、無力化するアクションを開始
- 再発するインシデントの根本原因に対処するための実用的なアドバイスを提供

たとえお客様の組織に成熟したセキュリティ運用センターがあったとしても、脅威がすり抜けて侵入しないように別の角度から環境を監視することが必要かもしれません。Sophos MDR は、脅威ハンティングとエンドポイント保護を統合すると同時に、日々の監視と専門知識を提供します。お客様のネットワークとクラウドアセットは、ソフォスのネットワークアナリストと脅威ハンターにとって最優先事項です。これらのアナリストが、お客様に代わって脅威を監視し、積極的に修復・無効化します。

適切な MDR サービスを使用すると、組織を常に監視し、脅威を探し出し、疑わしいアクティビティを調査し、潜在的なインシデントに対応する熟練した専門家チームがいるので、ご安心いただけます。サイバーセキュリティの脅威の傾向は増え続けているため、サイバーセキュリティに重点を置いているチームと連携することで、安心感が得られます。

Sophos MDR が貴社をどのようにサポートするかについては、ソフォス営業担当者に問い合わせるか、コールバックをリクエストしてください。それまでの間、最新の MDR リサーチと事例をご確認ください。

ソフォス株式会社営業部
Email: sales@sophos.co.jp

22-08-08 WP-JA (PC)