SOPHOS
Cybersecurity delivered.

インシデント対応の専門家からの 4つの重要なヒント

重要なサイバー攻撃への対応方法を事前に把握

深刻なサイバーインシデントに対応することは、ストレスが非常にかかり、時間もかなり費やすことになります。攻撃に対処するプレッシャーを完全に軽減することはできませんが、インシデント対応の専門家からのこれらの重要なヒントを把握しておくことで、組織を守る際にチームが優位な立場になることができます。

このドキュメントでは、サイバーセキュリティのインシデントへの対応に関して、誰もが学ぶべき最大の教訓について説明します。数千件ものサイバーセキュリティのインシデントに連携して対応してきた Sophos Managed Detection and Response チームと Sophos Rapid Response チームの実際の経験に基づいています。

ヒント 1：できる限り早く取り掛かる

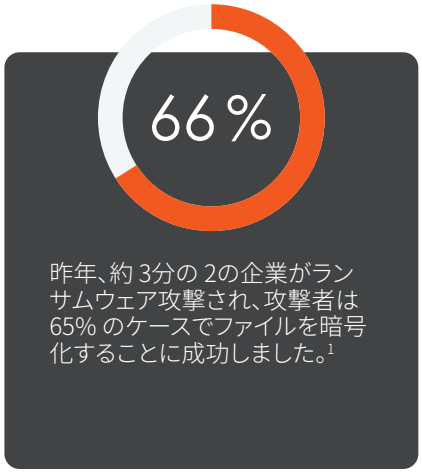
組織が攻撃を受けている時は、一刻を争います。

チームが取り掛かるのに時間がかかりすぎる理由はいくつかあります。最も一般的な理由は、自分自身が直面している状況の深刻さを理解していないこと、そして意識の低さが緊急性の欠如につながっています。

攻撃は、休日、週末、夜間など、最もタイミングの悪い時に発生する傾向があります。 ほとんどのインシデント対応チームでは人員がかなり不足していることは理解できますが、「明日、取り掛かりましょう」という態度につながる可能性があります。しかし残念ながら、明日になってから攻撃の影響を最小限に抑えようとしても遅すぎるかもしれません。

また、困惑したチームは、警告疲れにも悩まされるため、攻撃の指標への反応が遅くなる可能性が高くなります。これにより、シグナルが意味を失うことになります。最初にケースが作成された時でも、可視性とコンテキストが不足しているため、正しい優先順位が付けられない可能性があります。これでは、時間がかかります。しかし、インシデント対応では、防御側には時間がありません。

セキュリティチームが攻撃を受けていることに気付いて、すぐに何かを実行する必要がある状況にいたとしても、次に何をすべきか分からず、そのため対応に時間がかかる場合もあります。これに対処する最善の方法は、あらかじめインシデントに対する計画をしておくことです。



ヒント 2：「ミッション達成」をすぐに宣告しない

インシデント対応に関しては、症状を抑えるだけでは不十分です。その根本を治療することも重要となります。

脅威が検出された時にまず最初に実行することは、即時攻撃を優先順位付けすることです。これは、ランサムウェアの実行ファイルやバンキング型トロイの木馬をクリーンアップしたり、データの流出をブロックしたりすることを意味します。ただし、多くの場合、チームは最初の攻撃は阻止しますが、根本原因を実際に解決していないことに気付いていません。

マルウェアの削除と警告のクリアに成功したからといって、攻撃者が環境から排除されたわけではありません。また、検出されたものはただの攻撃者によって実行されたテストであり、どのような防御策を講じているかを確認しただけである可能性もあります。攻撃者がまだアクセスできる場合、攻撃者は再び攻撃をする可能性がありますが、さらに破壊的になるでしょう。

インシデント対応チームは、軽減した最初のインシデントの根本原因を確実に対処する必要があります。攻撃者はまだ環境に足掛かりがありますか？攻撃の第 2 波の開始に準備していますか？何千もの攻撃を修復してきたインシデント対応オペレーターは、より深く調査するタイミングと場所を把握しています。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、それらも無効化します。

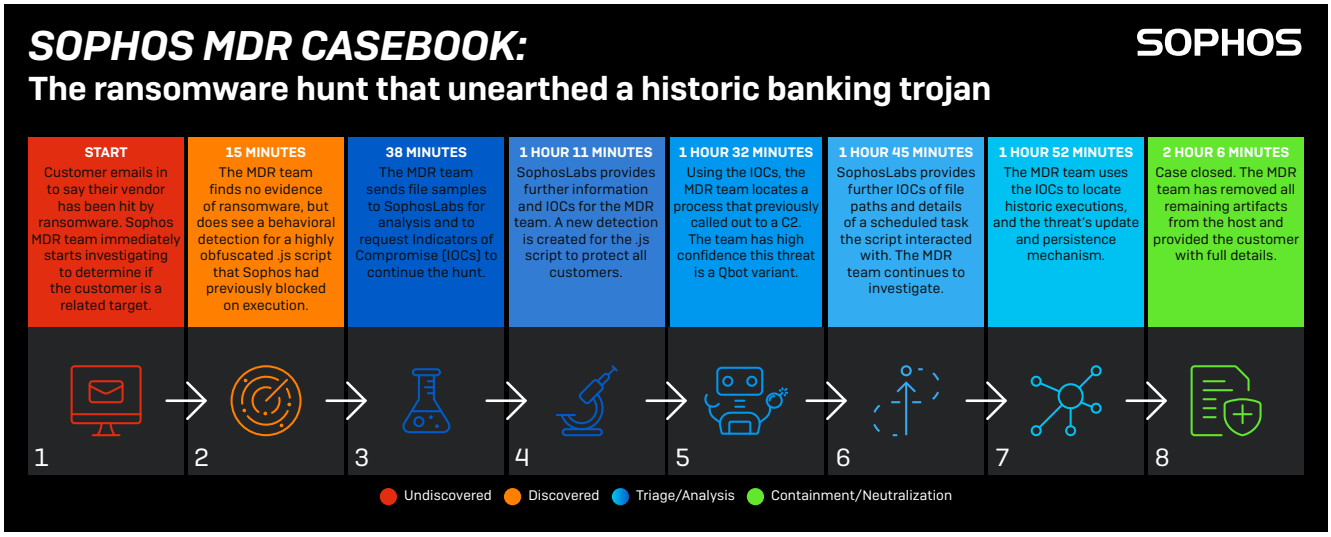
たとえば、ある例では、ソフォスのインシデント対応スペシャリストは、9日間続く攻撃を阻止し、攻撃者がランサムウェアで組織に 3回の別々の攻撃を試みるのを確認しました。

Sophos MDR サービスを利用しているお客様ではないため、まず Sophos Rapid Response チーム が初動対応しました。

攻撃の第1波 (最終的には組織のエンドポイント保護ソリューションによりブロックされた) では、攻撃者は、Maze ランサムウェアを使用して 700台のコンピュータを標的にし、1500万米ドルの身代金要求を行っていました。標的対象となった企業のセキュリティチームは、攻撃を受けていることに気付いたので、Sophos Managed Detection and Response (MDR) チームの高度なインシデント対応スキルを活用しました。

ソフォスのインシデント対応スペシャリストは、侵害された管理者アカウントを即座に特定し、悪意のあるファイルを特定して削除し、攻撃者のコマンドと C2 (コマンド&コントロール)通信をブロックします。その後、Sophos MDR チームは、攻撃者による 2つの追加攻撃の波から防御することが出来ました。もしも、攻撃者が成功し、被害者が支払いを済ませていたら、これは今までで最も高額なランサムウェアの支払いの 1つとなった可能性があります。

別の例では、Sophos MDR チームは潜在的なランサムウェアの脅威に対応しましたが、すぐにランサムウェアの証拠がないことに気付きました。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、悪名高いバンキング型トロイの木馬を発見しました。このお客様にとって幸いなことに、脅威はもはやアクティブではありませんでした。しかし、より広範な攻撃の指標となる可能性があるため、根本原因を完全に特定するために初期症状の後にやってくる状況を見越すことがなぜ重要であるかという一例として役立っています。



ヒント 3:完全な可視性が非常に重要

攻撃を受けている最中でも、何も見ずに行動することほど、組織を守ることを難しくするものはありません。攻撃の潜在的な指標を正確に特定し、根本的な原因を特定することを可能にする、適切な高品質のデータにアクセスすることが重要です。

優れたチームは、シグナルを確認するために適切なデータを収集し、ノイズからシグナルを分離し、どのシグナルが最も重要で優先順位が高いかを知ることができるのです。

シグナルの収集

環境の可視性が制限されていると、攻撃を確実に見逃すことになります。長年にわたり、多くのビッグデータのツールが、この特定の課題を解決するために市場に投入されてきました。ログイベントのようなイベントベースのデータに依存するものもあれば、脅威ベースのデータを利用するもの、そしてハイブリッドアプローチに依存するものもあります。いずれにしても、目標は同じです。十分なデータを収集して、それ以外の方法では見逃されていたであろう攻撃を調査および対応するのに重要な情報を生成します。

さまざまなソースから適切で高い質のデータを収集することで、攻撃者の TTP (ツール、戦術、および手順) を完全に可視化できます。そうしないと、攻撃の一部しか把握できない可能性があります。

ノイズの軽減

攻撃の全体像を把握するのに必要なデータが揃っていないことを恐れて、一部の組織 (および組織が信頼しているセキュリティツール) はすべてを収集します。しかし、すべてのデータを収集することは簡単ではありません。必要以上にデータを集めることで本当に必要なものを見つけるのが難しくなっています。これにより、データ収集とストレージの費用が増加するだけなく、多くのノイズも発生し、警告による疲弊と誤検出の追跡に費やす無駄な時間が発生します。

コンテキストの適用

脅威の検出と対応専門家の間では、次のような格言があります。「コンテンツは王様だが、コンテキストは女王様だ」。両方とも、効果的なインシデント対応プログラムを実行するには必要です。シグナルに関連した意味のあるメタデータを適用することで、アナリストはそのようなシグナルが悪意のあるものか無害なものかを判断できます。

効果的な脅威検出と対応の最も重要な要素の 1つは、最も重要なシグナルに優先順位付けすることです。最も重要な警告を特定する最善の方法は、セキュリティツール (EDR ソリューション)、AI、脅威インテリジェンス、および人間のオペレーターの知識ベースによって提供されるコンテキストの組み合わせです。

コンテキストは、シグナルの発信元、攻撃の現在の段階、関連したイベント、およびビジネスへの潜在的な影響を特定するのに役立ちます。

ヒント 4：サポートを依頼する

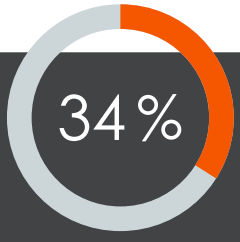
どんな組織も、インシデント対応をしたいと思う組織はありません。しかし、インシデント対応に関しては、対応経験に勝るものはありません。大きなプレッシャーがかかるインシデント対応に取り組むことが多い IT チームとセキュリティチームは、単に対処するスキルがないという状況、つまり、ビジネスに甚大な影響を与えるという状況にたびたび置かれます。

インシデントの調査や対応をする熟練した人材の不足は、今日のサイバーセキュリティ業界が直面している最大の問題の一つです。この問題は広く蔓延しており、ESG Research2 によると、「最大の課題は、根本原因や攻撃チェーンを特定するエンドポイントなどのサイバーセキュリティインシデントを調査できるスキルのある人材が不足していると答える人が 34% いる」ことが分かりました。

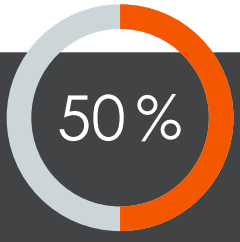
このジレンマは、マネージド セキュリティ サービスという新しい代替手段により解決できます。具体的には、Managed Detection and Response (MDR) サービスです。MDR サービスは、スペシャリストのチームが提供する外部委託されたセキュリティ運用であり、お客様のセキュリティチームの拡張として機能します。このサービスは、アナリスト手動の調査、脅威ハンティング、リアルタイム監視、インシデント対応をテクノロジースタックと組み合わせて、インテリジェンスを収集、および分析します。Gartner によると、「2025 年までに、組織の 50% が MDR サービスを使用するようになっている」3、と述べており、このことは、組織が、完全なセキュリティ運用とインシデント対応プログラムを実行するためには支援が必要であることに気付いているという傾向を示しています。

MDR サービスを採用しておらず、積極的な攻撃に対応している組織にとって、インシデント対応スペシャリストのサービスは最適なオプションです。インシデント対応担当者は、セキュリティチームが圧倒され、外部の専門家を必要とするときに動員され、攻撃の優先順位付けし、攻撃者を無力化にします。

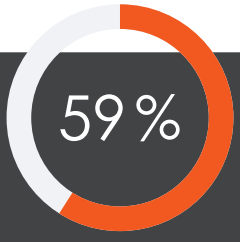
熟練したセキュリティアナリストを揃えたチームを持つ組織でさえ、カバレッジ (夜間、週末、休日など) のギャップを埋めたり、インシデントに対応する時に必要な専門的な役割を補うためにインシデント対応サービスと協力することでメリットを得ることができます。



アナリスト調査会社である ESG によると、「最大の課題は、根本原因や攻撃チェーンを特定するエンドポイントなどのサイバーセキュリティインシデントを調査できるスキルのある人材が不足している」と組織の 34% が答えています。[2]



2025 年までに、組織の 50% が MDR サービスを使用するようになります (これは 2019 年より 5% 弱増加しています)。[3]



5,600人の IT 専門家を対象とした 2022年の調査では、59% の回答者が、組織に対する攻撃の複雑さが昨年よりも増加したと述べています。[4]

ソフォスが提供する支援

Sophos Managed Detection and Response (MDR) サービス

潜在的に深刻となる可能性のあるインシデントの対応に組織の能力についての懸念はありますか？ その場合は、Sophos Managed Detection and Response (MDR) サービスを検討する価値があります。

Sophos MDR とは、脅威ハンティング、検出、対応機能を 24時間 365日でソフォスの専門家チームより提供するフルマネージド型サービスです。(ご注意、2022年4月下旬より日本語翻訳サービスでの対応が可能となる予定です。)Sophos MDR チームは、単に攻撃や疑わしい挙動を通知するだけではなく、組織に代わって標的を絞って対処し、最も高度で複雑な脅威であっても無効化します。インシデントが発生した場合、MDR チームはリモートで脅威を阻止、封じ込め、無力化するためのアクションを開始します。セキュリティ運用の専門家チームは、再発するインシデントの根本原因に取り組むための実用的なアドバイスも提供します。

詳細はこちら www.sophos.com/mdr

Sophos Rapid Response サービス

組織が攻撃を受け、迅速なインシデント対応の支援を必要としている場合は、ソフォスがサポートします。

Sophos Rapid Response は、インシデント対応担当者の専門家チームによって提供され、組織に対してアクティブな脅威の特定と無効化を迅速に支援します。(日本語通訳サービスを利用できます。)オンボーディングは数時間以内に開始され、ほとんどのお客様は 48時間以内に優先順位付けされます。このサービスは、ソフォスの既存のお客様とソフォス以外のお客様の両方が利用できます。

リモートインシデント対応担当者である Sophos Rapid Response チームは、速やかに脅威を優先順位付け、封じ込め、無力化を実行します。お客様の資産のさらなる損害を防ぐために組織から脅威が追放されます。

詳細はこちらwww.sophos.com/rapidresponse

Sophos XDR

Sophos XDR は、ネイティブのエンドポイント、サーバー、ファイアウォール、メール、クラウド、M365 セキュリティを同期する業界唯一の XDR ソリューションです。専用の SOC チームと IT 管理者ともに、脅威検出、調査、対応のための豊富なデータセットと詳細な分析を使用して、組織の環境の全体像を把握できます。

詳細と無償評価版はこちらからwww.sophos.com/xdr

[1] ランサムウェアの現状 2022年版 - 31 か国、5,600 人の IT 管理者を対象としたベンダーに依存しない独立調査に基づいています: https://www.sophos.com/ja-jp/whitepaper/state-of-ransomware
[2] https://www.esg-global.com/blog/soapa-discussion-on-edr-and-xdr-with-jon-oltsik-and-dave-gruber-video-part-1
[3] ガートナー社、Market Guide for Managed Detection and Response Services、2020 年 8月 26日、アナリスト：Toby Bussa、Kelly Kavanagh、Pete Shoard、John Collins、Craig Lawson、Mitchell Schneider
[4] ランサムウェアの現状 2022年版 - 31 か国、5,600 人の IT 管理者を対象としたベンダーに依存しない独立調査に基づいています: https://www.sophos.com/ja-jp/whitepaper/state-of-ransomware

ソフォス株式会社営業部
Email: sales@sophos.co.jp

22-08-08 WPJA (PC)