SOPHOS

EDR が必要な 5 つの理由

EDR (Endpoint Detection and Response) ツールは、エンドポイントセキュリティの検出 / 調査 / 対応機能を強化・補足します。しかし、EDR ツールに対する過剰な期待が広まるなか、その具体的な使用方法や必要となる理由を把握するのは容易ではありません。さらに悪いことに、企業が EDR ソリューションを導入しても、しばしば、使いにくい、十分な保護機能がない、リソースに過大な負荷を与える、などの理由で価値をもたらすことが困難になっています。

Sophos Intercept X with EDR は、高度な EDR 機能と、業界トップレベルのエンドポイントとサーバー保護機能を単一のソリューションとして統合し、セキュリティインシデントに関する複雑な問題に企業が容易に対処することを可能にしています。EDR ソリューションの導入を検討するにあたっては、以下で説明するメリットも考慮してください。

IT セキュリティの運用の予防状態を維持し、ステルス型の脅威を阻止します。

組織に応じて、IT 運用と IT セキュリティ担当者は、同じチームの一員になることも、独立して運用することも、同一の担当者になることもできます。どのような設定を行う場合でも、2つの領域で EDR ツールとは異なるユースケースを必要とするため、ツールは両方のタスクセットを実行でき、電源を落とさずにアクセス可能である必要があります。

IT 運用管理者にとって、組織全体を健全な状態に保つことは非常に重要です。たとえば、ディスク容量が少ない、メモリ使用量が多いなどのパフォーマンスの問題があるマシンを検索します。パッチの適用を必要する脆弱なプログラムが存在するデバイスを検索します。RDP が不必要に有効になっている、もしくはゲストカウントが有効になっているエンドポイントとサーバーを追跡します。Sophos EDR では、管理者にこれらのすべての質問やそのほかの質問をするツールを提供する以外にも、パフォーマンスの問題の調査、パッチのインストール、RDP およびゲストアカウントの無効化をすることでデバイスにリモートアクセスをしてセキュリティホールを修正します。

サイバーセキュリティの専門家は、エンドポイント保護によって自動的には検知されない掴みどころがなく回避型の脅威を探し出す必要があります。EDR ツールは、感染の痕跡 (IoC) を効率的に追跡する必要があります。たとえば、非表示ポートで接続しようとするプロセス、ファイルやレジストリキーを編集したプロセス、他の何かになりすましているプロセスを特定、フィッシングメール内のリンクをクリックした従業員を追跡などです。Sophos EDR を使用すると、これらのタイプの調査を組織全体で迅速に実行することができます。その後、目的のデバイスにリモートからアクセスして、より深く掘り下げ、フォレンジックツールを導入し、疑わしいプロセスを終了することも簡単です。

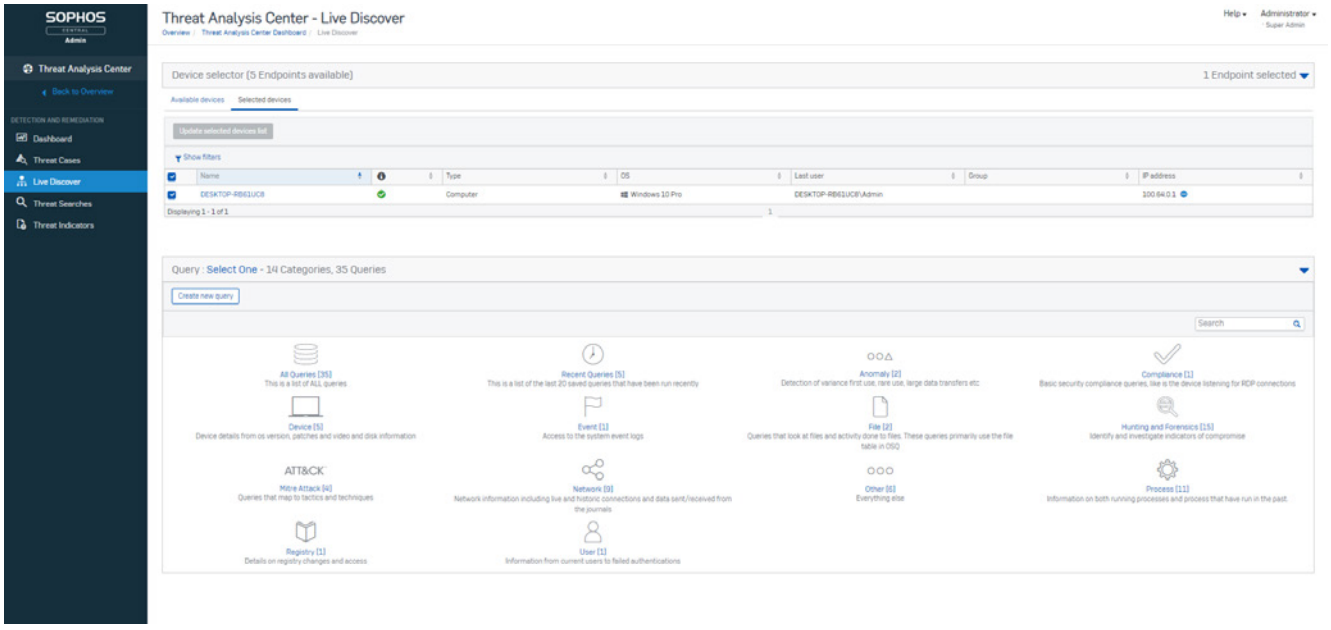

図1：Sophos Intercept X with EDR を使用すると、ユーザーは組織全体にわたり詳細な質問をすることができます

これまで検出されていなかった攻撃を検出

たとえ高度なサイバー セキュリティ ツールであっても、攻撃者が時間とリソースを投入すれば、いずれそれを破ることができます。したがって、これは攻撃が発生しても、状況を正確に把握するのが難しいことを意味します。企業はセキュリティ対策として、しばしば予防のみに依存します。もちろん予防は重要ですが、EDR はこれまで検出されていなかったインシデントを検出することで別の保護レイヤーを提供します。

企業は、EDR を活用して IOC (感染の痕跡) を検索することで攻撃を検出できます。これによって、これまで検出されていなかった攻撃を迅速かつ簡単に検出できます。企業の脅威検索は、第三者機関の脅威解析機関から通知を受けてから実行されることがよくあります。たとえば、US-CERT、CERT-UK、または CERT Australia などの政府機関が、ネットワークで疑わしい動作があることを企業に通知する場合などです。通知と共に IOC のリストが提供されることもあり、感染の状況を解明する出発点としてそれを使用することができます。

Intercept X の脅威インジケータ機能は、上位の疑わしいイベントのリストを生成し、それに基づいて IT / セキュリティ管理者は、調査が必要なイベントを特定することができます。脅威スコアでランキングされる上位の疑わしいイベントのリストは、SophosLabs の機械学習機能を活用して生成されます。これを基に IT / セキュリティ管理者は、必要な作業に優先順位を付け、最も重要なイベントに集中できます。

どこから開始するかを把握することで、アナリストは組織全体にわたって疑わしいアイテムのすべてのインスタンスを追跡し、迅速にクリーンアップするためのアクションを実行できます。さらに、強力な SQL クエリを活用して、レジストリキーを編集するプロセスや非表示ポートに接続しようとするプロセスなど他の感染の痕跡を追跡できます。

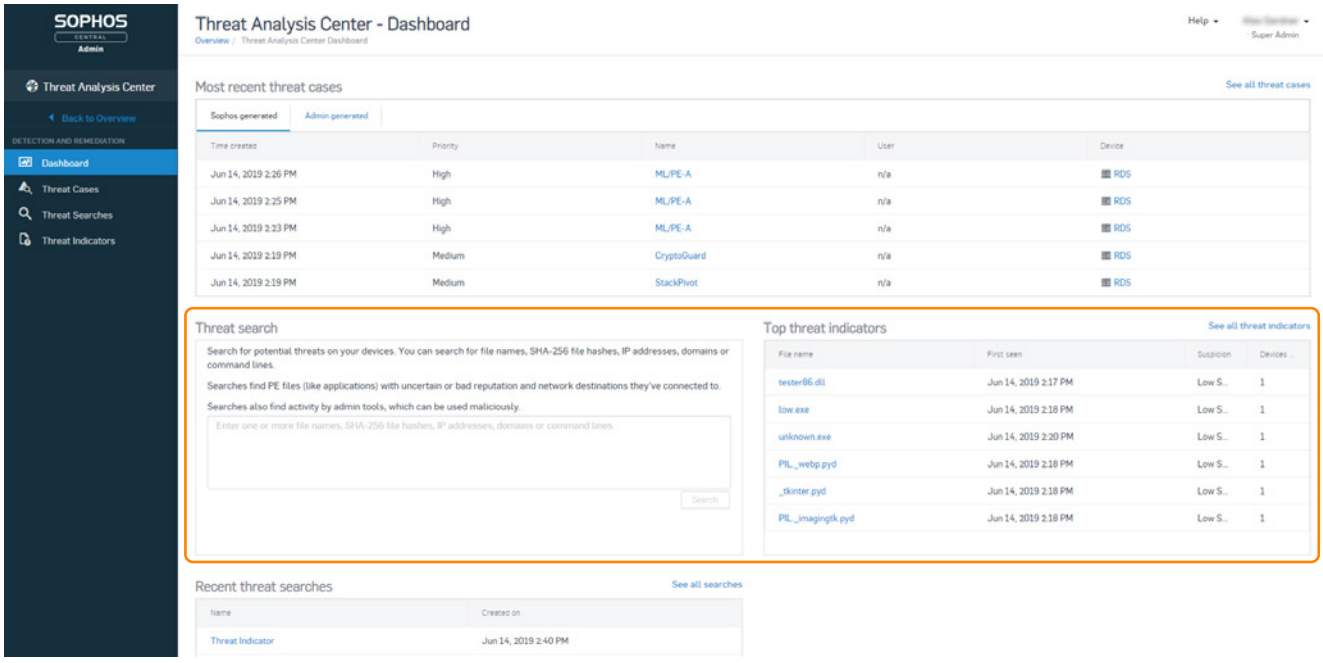

図2：Sophos Intercept X with EDR は、ネットワーク全体で 感染の痕跡 (IoC) を検索できます。また、機械学習も活用して、調査が必要な上位の疑わしいイベントを決定できます

詳細な質問を行う機能と、どこから開始するかのガイダンス、および収集された脅威インテリジェンスを組み合わせることで、管理者はすべての長所を生かすことができ、電力や精度を犠牲にすることなく簡単に Sophos EDR を使用できます。

潜在的インシデントへの対応の迅速化

IT / セキュリティ管理者は、通常インシデントが検出されると、攻撃拡大のリスクを削減したり、被害を最小限に抑えたりするため、なるべく早く修復しようとします。当然のことながら、ここでの最重要課題は、脅威をそれぞれどのように排除するかです。IT / セキュリティ管理者は、各インシデントの修復に平均で 3時間以上を費やしています。EDR はこれを大幅にスピードアップできます。

インシデントレスポンスの第一のステップとして、IT / セキュリティ管理者は、攻撃の拡大を阻止しようとすることが考えられます。Intercept X with EDR は、ネットワークでの脅威拡大を防ぐ主な手順として、エンドポイントとサーバーをオンデマンドで隔離します。IT / セキュリティ管理者は調査を開始する前に、しばしばこの操作を実行して、最適な対策を打つ時間を確保します。

調査は時間がかかり、困難を伴うことがあります。もっとも、これは実際に調査が行われた場合の話で、行われないこともあります。従来のインシデントレスポンスは、IT / セキュリティ管理者の持つスキルに大きく依存します。また、大抵の EDR ツールでも、解析方法の選択や結果の解釈には、IT / セキュリティ管理者のスキルに大きく依存します。一方、Intercept X with EDR を使用すると、事前設定された手順に従って調査を実施できるので、専門知識のレベルを問わず、すべての IT / セキュリティ管理者が、企業のセキュリティインシデントにすばやく対処できます。製品に搭載された専門知識のデータ、推奨される次のステップや、わかりやすい視覚的な攻撃経路などが表示されます。

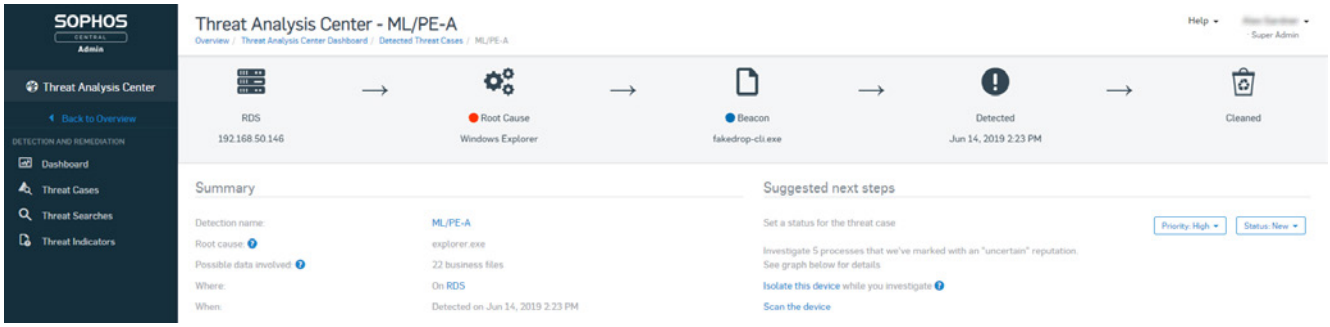

図3：手順に従ってインシデントに対応する機能では、推奨される次のステップが表示され、エンドポイントをオンデマンドで隔離できるので、迅速かつ安全にインシデントに対処できます。

Sophos EDR には、コマンドライン インターフェースを介してデバイスにリモートアクセスする機能も含まれています。従業員がオフィスに勤務していない場合でも、迅速な対応をするのに最適です。デバイスにアクセスすると、管理者は、フォレンジックツールの導入、ソフトウェアのインストール / アンインストール、プロセスの終了、デバイスの再起動によってさらに調査を行うことができます。

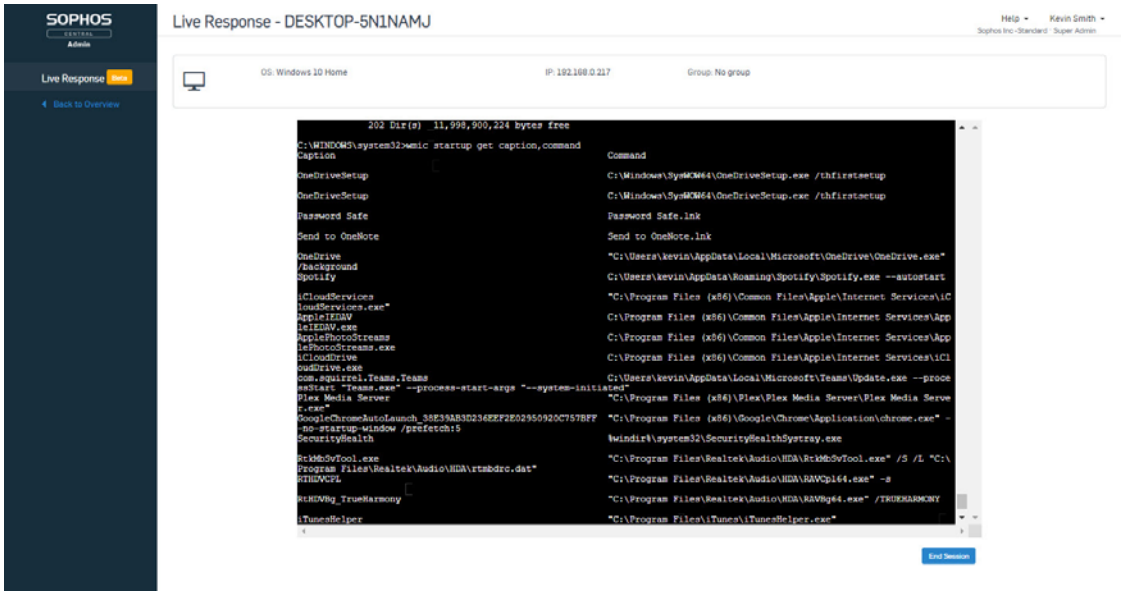

図4：Intercept X with EDR の複数の画面で「アクション」ボタンを使用できます。アクションの画面では、最も頻繁に表示される「クリーン&ブロック」ボタンなど、複数の復旧オプションを選択できます。

人的リソースを追加せずに、専門知識を獲得

EDR (Endpoint Detection and Response) 機能を追加しようとする企業が、その導入にあたり、他の障害と大差で、最も大きな障害として挙げるのは「スタッフのスキル不足」です。これは大きな驚きではないはずです。適切なスキルのあるサイバーセキュリティ専門家が見つからないことは、ここ何年かで広く話題になっています。このスキルギャップは、特に小規模企業で深刻です。

企業が EDR を導入していない上位の理由

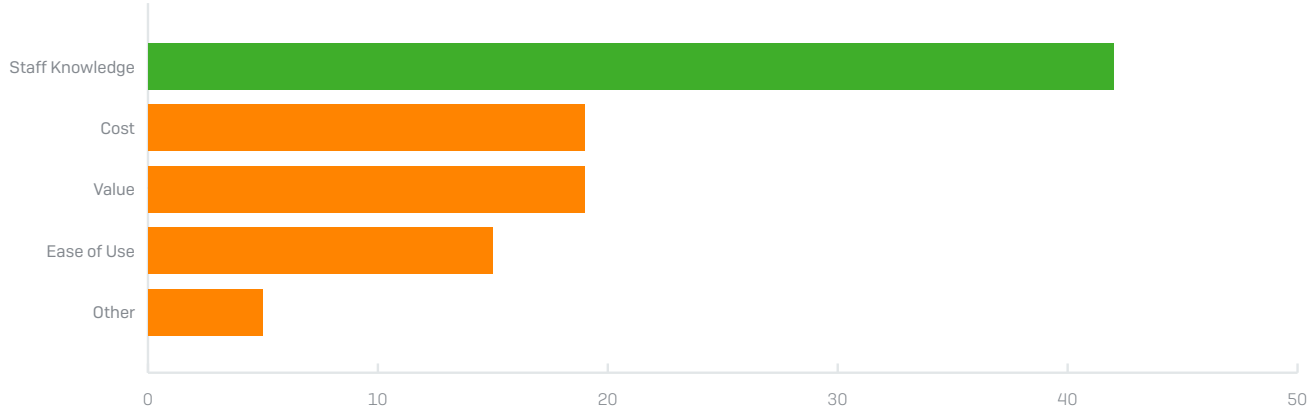

図5：企業が EDR (Endpoint Detection and Response) ソリューションを導入していない理由の最上位として「スタッフのスキル不足」が挙げられます
(出典：Sapio 社とソフォス共同の調査、2018年 10月)

Intercept X with EDR は、スタッフのスキルギャップに対応するため、本来アナリストによって提供されるスキルを、機能として搭載しています。EDR は機械学習を活用して、セキュリティの詳細な状況を把握し、SophosLabs がまとめた脅威解析情報で強化されています。したがって、人的リソースを追加することなく専門知識を獲得することができます。高度な EDR 機能は、スタッフのスキルギャップを埋め、これまでアナリストによって提供されていた以下のような専門知識を搭載しています:

- セキュリティアナリスト：インシデントを優先付けし、即座に対処が必要な警告を特定する、第一線のアナリストです。また、理想的には、これまで検出されていなかった攻撃をプロアクティブに検出することもできます。Intercept X with EDR は、脅威の疑いのあるイベントを自動的に検出し、優先順位を付けます。疑わしいイベントは、機械学習を使用して検出され、脅威スコアが与えられます。スコアが高いイベントほど、即座に対処が必要であることを意味します。したがって、IT / セキュリティ管理者は、即座に対処が必要なイベントを直ちに見極めて、調査を開始することができます。
- マルウェアアナリスト：企業は、マルウェア解析の専門家が行う、疑わしいファイルのリバースエンジニアリングによる解析に依存する場合があります。しかしこの方法は、時間がかかり難しいだけでなく、大抵の企業にはない高レベルのサイバーセキュリティの専門知識を前提としています。マルウェアアナリストは、ファイルがブロックされなかったが、実際は悪質であるかどうかを判断する必要があります。また、悪質であると判断されたファイルが誤検出である可能性を調査する必要もあります。Intercept X with EDR は機械学習を活用して、より優れた方法でマルウェア解析を実行します。業界トップレベルのエンドポイント用マルウェア検出エンジンを使用して、マルウェアの徹底した分析が行われ、ファイルの属性やコードのコンポーネントを細分化したうえで、他の無数のファイルと比較されます。IT / セキュリティ管理者は、どの属性やコードセグメントが、既知の「正規」ファイルまたは「不正」ファイルに似ているかを簡単に把握して、ファイルのブロック/許可を判定できます。

- 脅威解析アナリスト：調査にあたり、脅威の可視性と背景を提供するため、サードパーティーの脅威解析情報 (しばしば追加コストが伴います) に依存する場合があります。脅威解析アナリストは、このデータを解釈・統合して、対策に生かす必要があります。脅威解析情報は調査の出発点として使用でき、疑わしいファイルについてセキュリティコミュニティに質問したり、攻撃が企業を対象にしているかどうかを判断したりするための手段として利用できます。Intercept X with EDR は、SophosLabs がまとめた脅威解析情報へのオンデマンドアクセスを IT / セキュリティ管理者に許可して、より詳細な情報を収集できるようにします。脅威の動向に関する詳細な情報を常に把握するため、SophosLabs は毎日およそ 40万件の未知・新種のマルウェアを追跡・分析・解析して、最新かつ最大の攻撃を常時検索しています。この脅威解析情報は収集、集約、要約された後、簡単な解析結果が生成されるので、専門の脅威解析アナリストがいない、または高価で理解が困難な脅威フィードへのアクセスのない IT / セキュリティ管理者でも、世界最高レベルのサイバーセキュリティの研究チーム、およびデータサイエンスチームの専門知識を活用することが可能になります。

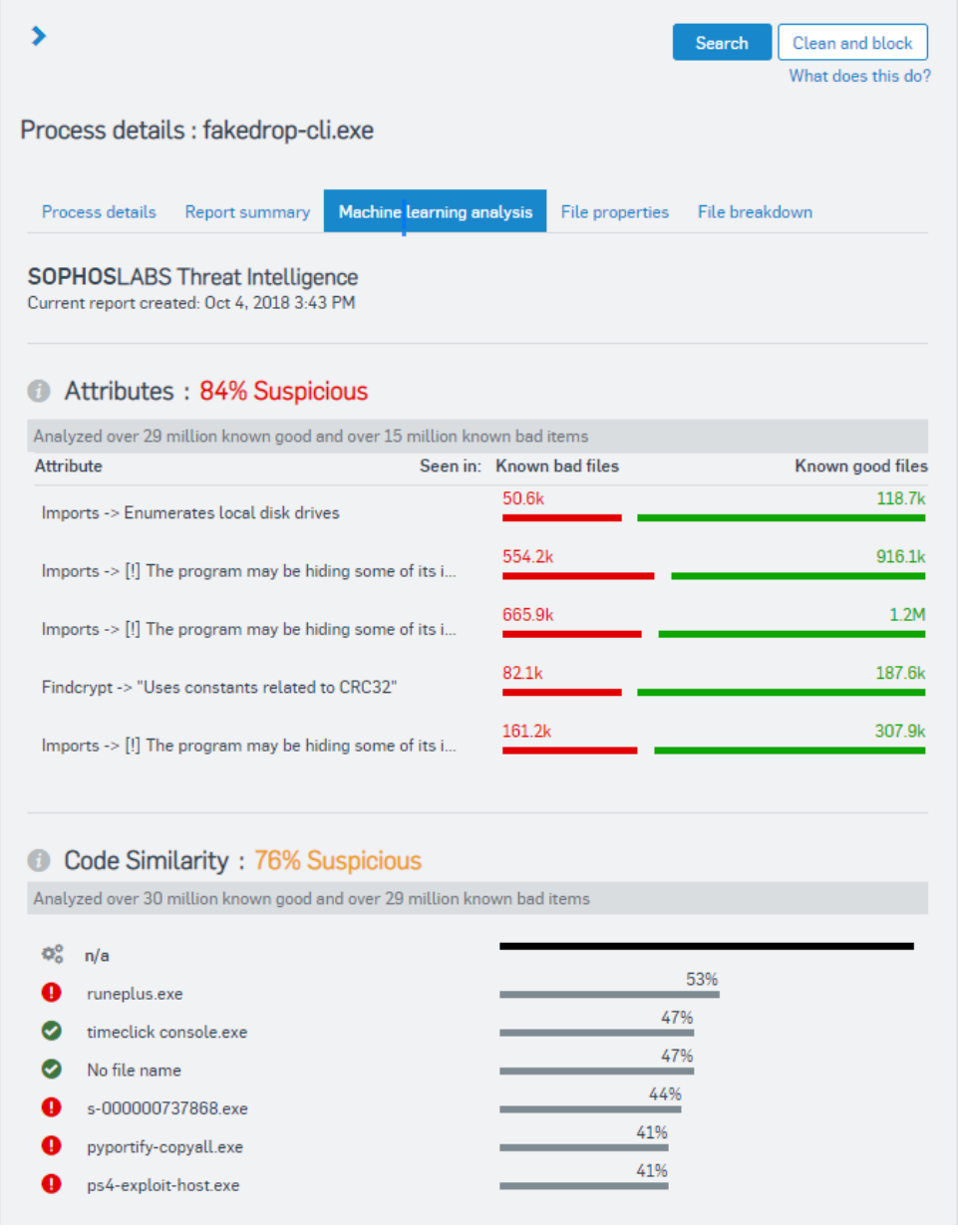

図6：機械学習分析は、属性、コードの類似性、ファイルパス分析を表示し、シンプルでパワフルな分析を行います。

Managed Threat Response (MTR)

EDR の管理に関するヘルプをお探しですか? Sophos MTR サービスはテクノロジーと専門家の分析を融合させることで、向上した脅威ハンティングおよび検出、より詳細なアラートの調査、洗練されて複雑な脅威を排除するように標的を絞った行動を取ります。

攻撃経路の解明と再発防止対策

繰り返し見る悪夢のように IT / セキュリティ管理者が想像する最悪の事態は、企業が攻撃を受けた際、上司に「なぜこのような事態が発生したのか？」と問い詰められても返答できない、という状況です。悪質なファイルを検出して除去することで当座の問題は解決しますが、マルウェアが最初にシステムに侵入した経路や、検出・除去されるまでに実行された動作は明らかになりません。

Intercept X with EDR にある脅威ケースは、感染を引き起こしたすべてのイベントを表示するので、マルウェアがアクセスしたファイルやプロセス、レジストリキーを把握して、攻撃範囲を判断することができます。攻撃チェーン全体を視覚化して表示するため、攻撃経路および攻撃範囲を正確に把握することができます。さらに重要な点として、IT / システム管理者が攻撃の根本原因を理解することで、再発を防止できる可能性が高くなります。

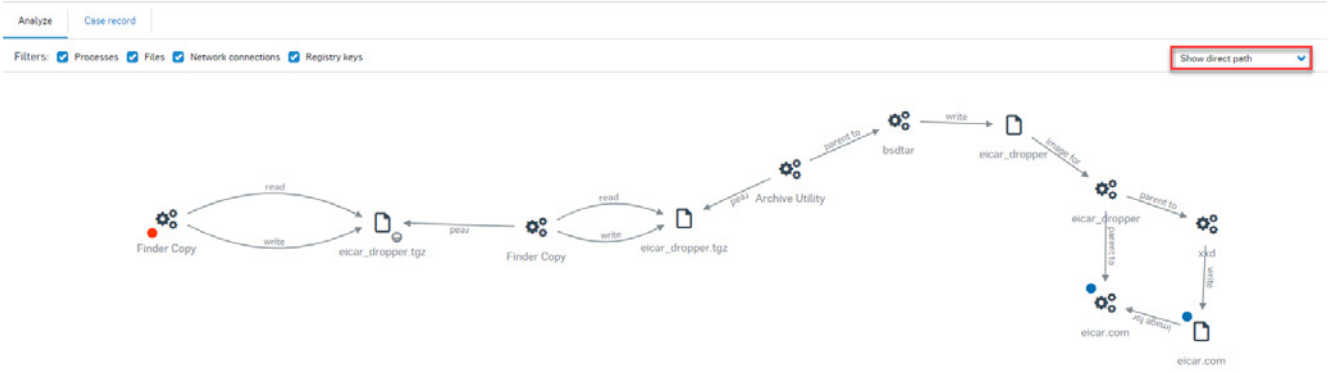

図7：脅威ケースは、インタラクティブな攻撃チェーンの視覚化を提供します。

サイバーセキュリティ環境全体の可視性

ソフォスは EDR と XDR (Extended Detection and Response) の両方を提供しており、エンドポイントやサーバー、ネットワークデータやメールデータなど、比類のない可視性を提供します。包括的な環境である全体像から、調査が必要な分野の詳細まで、すばやくピボットできます。これは、ランサムウェアなどの最新の脅威を阻止し、エクスプロイト技術をブロックし、ハッカーを阻止する業界最先端の保護機能となります。

詳細と無償評価版の開始についてはこちらから sophos.com/interceptx

無償評価版

無償評価版の登録 (30日間)
www.sophos.com/ja-jp/interceptx

ソフォス株式会社営業部
Email: sales@sophos.com

2021-04-19 (MP)

SOPHOS