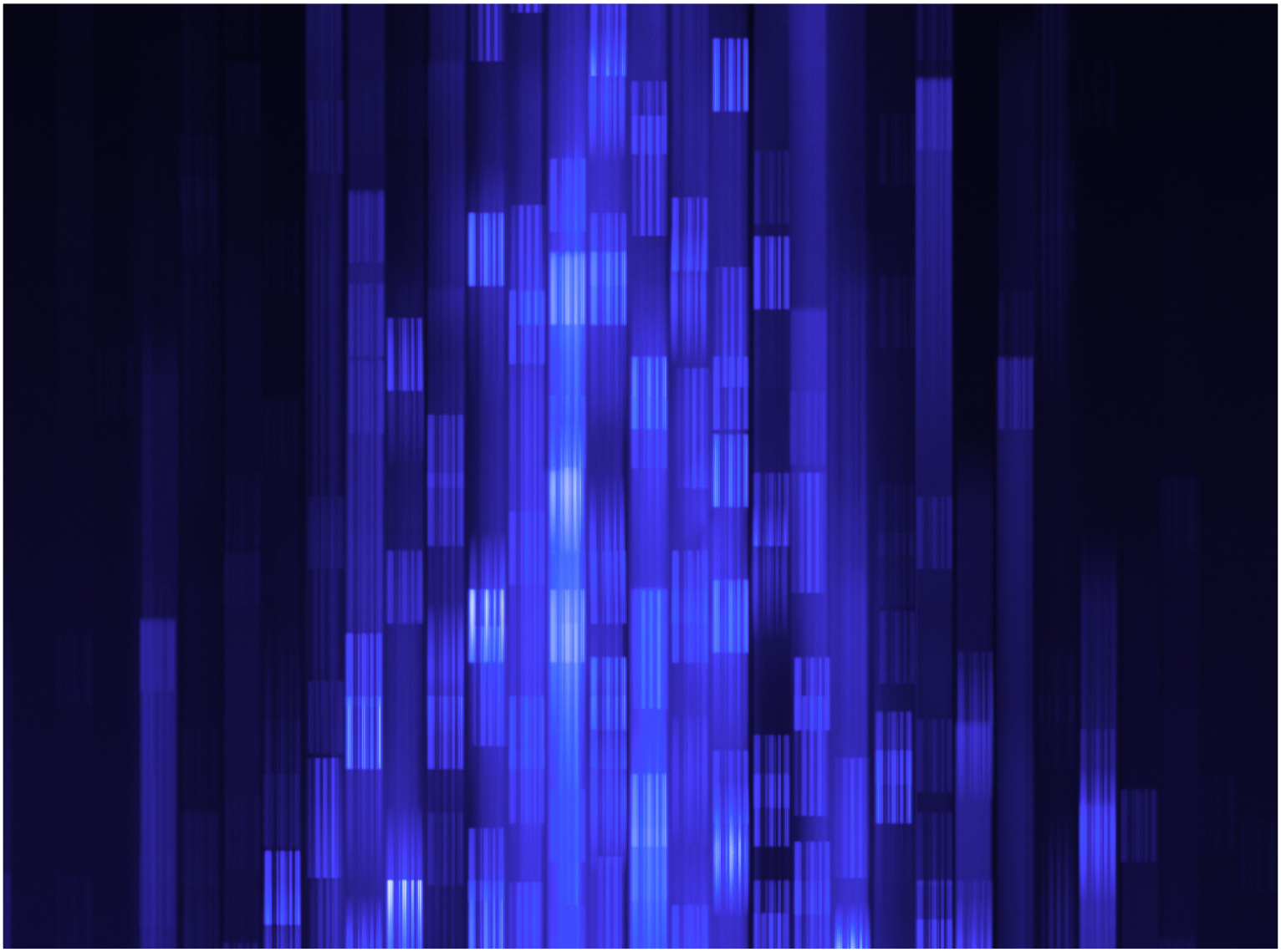
Secureworks

ホワイトペーパー

Counter Threat Unit™のリサーチャーに寄せられる7つの質問



1. 自社の業種を標的にしているのはどの脅威グループなんでしょうか？

悪意ある者を観察し、戦ってきた当社の経験について、セキュリティリーダーや担当者が質問したいことがたくさんあると思います。

攻撃者が組織を標的にしてに侵入を試みるには様々な理由があり、必ずしも単一の方向に焦点を当てているわけではありません。価値があるとみなされるものを作ったり、価値のあるものにアクセスしたり、または価値のあるものを作ったりアクセスしたりする人と信頼関係にある組織は、すべて標的になる可能性がある、あるいはおそらく既に標的になっています。

特定の脅威グループに関する情報を、同じ業種の組織を標的にしていることが確認されていないからといって無視するのではなく、ITやITセキュリティの専門家は、「もしこの技術・戦術・手順（TTP）が自社への侵入に使われたらそれを検知できるだろうか」と自問する必要があります。

その理由には、当社のCounter Threat Unit（CTU）のリサーチャーは、標的とされた脅威への対応から得られたデータを使用して、攻撃者の活動パターンと傾向を分析しています。一例として、優先順位付けの問題では、Bronze Faculty（Secureworks™ の命名）に起因する侵入は、様々な業種で何度も企てられました。この調査の結果、Bronze Facultyが標的とする業種を次から次へと乗り換えていることが明らかになりました。

CTUのリサーチャーが観察したBronze Facultyの活動に関連するデータを例にすると、本日、特定の業種を襲った脅威グループが、翌日には新しい業種に鞍替えする可能性があることを示しています。組織は、自社とは異なる業種しか狙っていないようにみえるグループからの脅威を決して無視してはいけません。CTU のリサーチャーは、脅威グループの TTP をセキュリティ対策を慎重に行い、有事に備えて可能な限り軽減戦略を事前に計画しておくことを推奨しています。

セキュアワークスのCounter Threat Unit™（CTU）は、サイバー脅威への対抗に関する専門知識を持つ85人以上のトップクラスの脅威リサーチャーで構成されています。セキュアワークスのオペレーションとサービスのすべてをサポートする、CTUが開発したインテリジェンスです。

2. どうすれば脅威から防御に成功できたといえるのでしょうか？

攻撃者は、お客様が防御に成功したことを自ら教えてくれます。当社の経験から、攻撃者は最初に排除されたことに気付くと、必ずまた同じ環境に戻ってきます。攻撃者を追い出し、再び環境への侵入を試みたことを俯瞰することができれば、防御に成功したという明確な合図と言えます。

他にも防御の成功を示す一般的な指標には、下記が挙げられます

- 検知までの時間が短縮できた
- レスポンスの時間を短縮できた
- 将来的に攻撃者と対抗するための組織力が向上した

Availability varies by region. ©2018 SecureWorks, Inc. All rights reserved.

この最後の項目については、次ページの図のように、他のグループにずっと乗っ取られ続けないようにすることを示しています。脅威からの防御するには、お客様の環境、アプリケーション、データを悪用し、ますます高度化するグループに、自社組織が対抗できることも意味します。

3. 防御の成功はどのように可視化できますか？

環境内に存在する脅威を認識したあるお客様の例をご紹介します。このお客様は当社のインシデント対応チームと 2 か月間協力してセキュリティ体制とフォレンジックの事前準備を改善し、様々な計画を同時に実行することで、すべての脅威グループを排除することができました。

お客様は、保護に対する計画と対策の重要性を認識し、当社のセキュリティリスクコンサルタントが、定期的に環境を評価する継続的なコンサルティング契約を進めることにしました。次の侵入は（5 か月ではなく）4 日後に確認されました。そのため、前回の契約からレスポンスのコストが大幅に削減されました。このお客様は、脅威グループが環境に侵入しようとする試みから解放されることは決してないものの、常に対応できることを理解されました。

4. どのタイミングで脅威に標的とされていると判断すればよいのでしょうか？

組織が脅威の標的となっているかどうかを最初から判断することは事実上不可能です。そのため、セキュリティチームはすべての脅威に狙われる可能性があると考える必要があります。この質問に答えるためには、組織は可視性、前後の状況、経験が必要です。

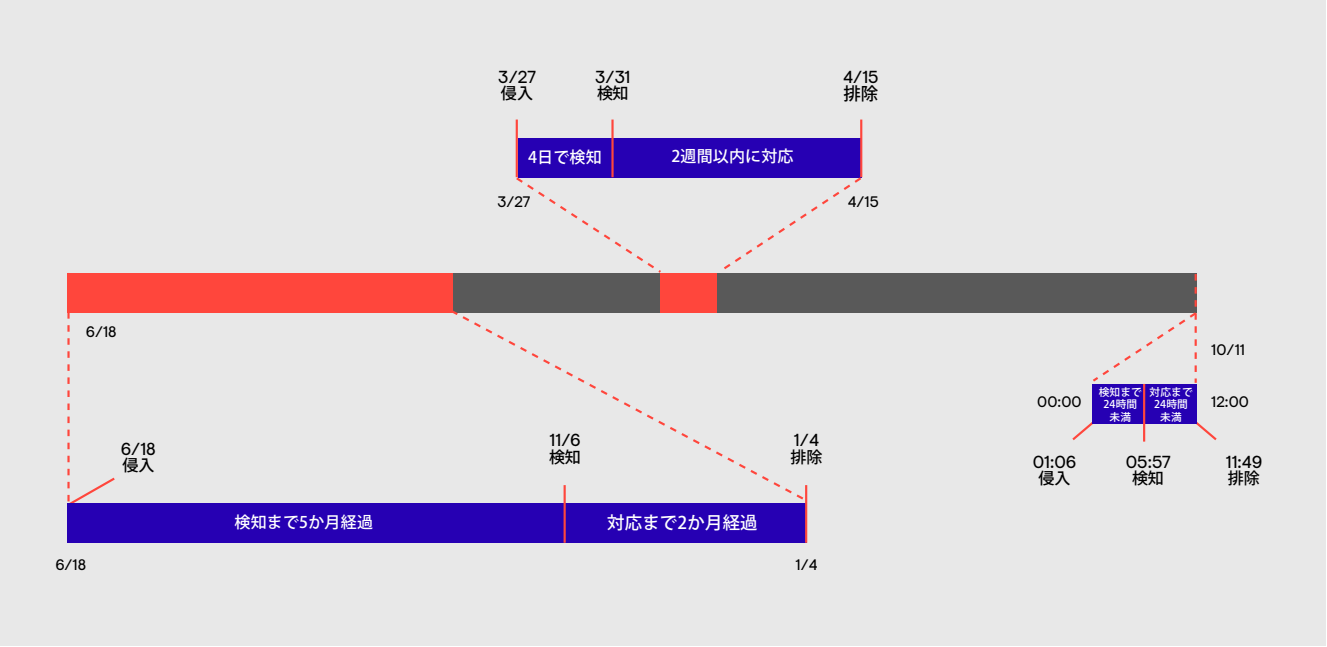
可視性

「標的」という用語は相対的なものであり、通常の「一般型」または「対象なし」の脅威とは異なります。何が「通常」であるかを理解するのは、境界内を可視化する設備しか持たない多くの組織にとっては困難なことです。

成熟度の高い組織では、セキュリティ組織による公開レポートや出版物で可視性を補完したり、信頼できるコミュニティに参加してメンバー間で脅威インテリジェンス情報を共有し、境界外の可視性を強化することが一般的です。しかしレポートやコミュニティの情報共有で可視化できるのは、そのコミュニティが観察できるものや、共有を許可されているものに限定されます。脅威に標的にされているかどうかを判断するのは、個々の組織が、そのスタッフが持つ可視性のレベルに基づいて判断しなければならず、大きな課題となります。

世界中に何千もの顧客が存在する MSSP モデルでは、様々な業種や地域のお客様に影響を与える脅威を観察します。この幅広い可視性により、脅威が全環境に共通する場合、特定の業種または地域に共通する場合、またはより的を絞った脅威として少数のお客様に固有である場合と、セキュアワークスが客観的に判断できるベースラインを提供します。

Availability varies by region. ©2018 SecureWorks, Inc. All rights reserved.



コンテキスト情報

すべての経営判断、特にリスクと脅威に関する経営判断には、特定の問題に対して、限られたリソース（時間、お金、人）をどのように配分するのかが重要です。コンテキスト情報は、正確かつ効果的な判断を行うための鍵であり、組織の可視性の成果でもあります。可視性が高くなるほど、攻撃の理解を深める情報量は多くなります。

セキュアワークスでは、その幅広い可視性を活用して、攻撃に関する過去のコンテキスト情報を含め、攻撃を包括的に理解し、「場当たり的」な攻撃と「標的型」攻撃の違いを特定します。過去のコンテキスト情報は、標的型攻撃には不可欠です。レスポンスチームは、攻撃と攻撃者がいつ、どのように侵入したか、攻撃者が何を設置した可能性があるか、攻撃者は環境内でどのように移動したか、そして最終的に攻撃者は目的（機密データの持ち出しなど）を実行し達成できたかを把握する必要があります。

当社は、数多くの標的型攻撃ハンティングとレスポンスの取り組みの中で攻撃者と向き合ってきたその経験から、当社のリサーチャーは攻撃者や攻撃グループの包括的なプロファイルを構築することで、上記の重要な問いに答え、理想的には攻撃者を防御できるように取り組んでおります。

経験

標的型攻撃の攻撃者は、人間的な要素があるため、他の攻撃者よりも複雑な敵です。この種の攻撃者はセキュリティ防御を回避し、目的を達成するまで検知されないまま環境にひたすら居座ろうとします。

Availability varies by region. ©2018 SecureWorks, Inc. All rights reserved.

Secureworks

セキュリティの専門家にとって、攻撃者の戦術・手法・手順（TTP）に対抗する経験を日々積んでおくことは重要です。経験によって、レスポンスチームはどうやって手掛かりが見つけられるのかを学び、点と点をつないで、最善の対応策を判断できるようになります。また、防御側からの反応をに気づいた攻撃者が、TTPを変化させたときにレスポンスチームが認識するのに役立つ、コンテキスト情報も提供されます。

当社の観点から見ると、新しいTTPを特定することで、リサーチャーが新しい検知・対応の方法を編み出して顧客ベース全体に展開し、脅威をより深く可視化できるようになります。これにより、リサーチャーは新しい情報を駆使して侵害の兆候を過去に遡って探し出し、境界内で何が起こっているのか気づかずに被害を受けていた当事者に知らせることができるようになります。

5. 予備知識がまったくない攻撃（いわゆる「未知の未知」）から組織をどうやって保護すればよいのでしょうか？

まず最初に行うことは、想定される動作とはどんな動作なのかを知るために、環境のベースラインを設定することです。自社のネットワークについて把握しておらず、何が良いのか、何が未知の可能性があるのかを識別できないというケースはよくあります。ネットワークに大量のノイズを発生させて、目立った動きをする攻撃グループもありますが、周到に既知の動作を真似したり、既存のITツールを利用して動作したりする攻撃グループもあります。例えば、企業のエンドポイント管理プラットフォームを使用して横展開し、コマンドを実行する攻撃者も見つかっています。

攻撃者のやり口を探すプロセスは、ネットワークやファイルの履歴などの既知の静的な基準を検索するだけではありません。従来のセキュリティ制御を回避しようとする攻撃者の思惑を探り、悪意ある目的を達成するための行動を識別する必要があります。

6. 今後 3〜5 年の新たなセキュリティ投資の最優先事項は何ですか？

答えは簡単、エンドポイントセキュリティです。エンドポイントコントロールは一時的な流行ではありません。このソリューションの特徴と統合はまだ進化していますが、そのコア機能（検知、フォレンジックの準備、レスポンス）を利用して、組織にエンドポイントへの窓口を提供し、侵害が疑われる場合の対応に必要な時間と労力も削減しますので、投資する価値があります。

Availability varies by region. ©2018 SecureWorks, Inc. All rights reserved.

7. 組織がセキュリティ体制を改善するためにできる3つのポイントとはなんですか？

情報資産の特定、ネットワークのセグメント化、および特権アカウントのアクセスと使用状況の監査において、明らかにに改善の余地が見られるポイントです。

まず組織は、情報資産を構成するもの、つまり、決して公にしたくないシステムとデータ、およびそれらが存在している場所を把握する必要があります。セキュリティチームが情報資産を特定できず、十分把握もしていない場合、強靭なセキュリティアーキテクチャを構築するのは非常に困難です。当社が関わる多くの組織は、「何が最も価値のある情報資産なのか」という質問に答えることができません。

次に、ネットワークのセグメント化です。ネットワークセグメンテーションにより、ユーザーからデータを分離し、さらにユーザーから重要資産を分離することができます。例えば、ワークステーションからサーバーをセグメント化したり、人事や財務などの管理・間接部門に関してネットワークトポロジをセグメント化することができます。

最後に、特権アカウントの使用状況の監査です。ドメイン管理者アカウントの数やその利用方法を把握していないため、特権をもつ攻撃者がその環境で自由に活動できてしまうという組織は多数存在します。活動を監視している組織の中には、「拒否」は記録しても「許可」は記録しないところもあり、そのどちらもを記録しなければいけません。

Availability varies by region. ©2018 SecureWorks, Inc. All rights reserved.

Secureworks®

セキュアワークス（NASDAQ:SCWX）は、デジタルで接続された世界で組織を保護するサイバーセキュリティのリーダーです。

当社は、何千もの顧客からの可視性を統合し、あらゆる場所のあらゆるソースからデータを収集して分析し、セキュリティ侵害の防止、リアルタイムでの悪意ある活動の検出、迅速な対応、そして新たな攻撃の予測を行います。当社は、お客様に「知識を集めて、もっとずっと安全な（Collectively Smarter. Exponentially Safer.™）」サイバー防御を提供します。

Corporate Headquarters

United States
1 Concourse Pkwy NE #500 Atlanta,
GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
UK House, 180 Oxford St
London W1D 1NN
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

日本
〒212-8589
川崎市幸区堀川町580
ソリッドスクエア東館20階
03-6893-2317
www.secureworks.jp

Availability varies by region. ©2018 SecureWorks, Inc. All rights reserved.