隠れた脅威を探す

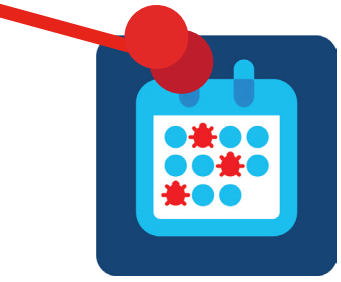
セキュリティ プログラムに脅威ハンティングを取り入れる

CISCO

目次

はじめに

時刻は昼の 1 時、すべてが順調です。昼食から戻ったシニア SOC 脅威研究者は、SIEM ダッシュボードでセキュリティ アラートがないか確認したばかりです。特にいつもと変わった点はありませんでした。最近の自動化プロジェクトによって、安全確認にかかる時間が大幅に短縮され、これまで手動タスクに費やされていた貴重な時間を活用できるようになりました。この空いた時間をどのように使いますか。



脅威ハンティングは、セキュリティ ポスチャを強化するためにあえて計画し、定期的に実施すべき業務です。

今こそ、脅威ハンティングを検討する絶好のタイミングです。脅威ハンティングでは、既知でない（つまり警告を受けたことがない）脅威を探します。セキュリティ ソフトウェアが警告できるのは、悪意のあることが判明しているリスクと振る舞いに限られます。それとは対照的に、脅威ハンティングでは未知の領域へと踏み込みます。

脅威ハンティングとは、感知されずに忍びこんだ攻撃者を見つけ出して根絶するための、能動的なセキュリティ業務です。危険性のあるアクティビティを検出した後の対応となる従来の調査や対策とは対照的です。

現状

先のシナリオが少し現実離れしているように見えるのは当然です。誰もが忙しいのに、午後に暇を持て余している人がいるでしょうか。

現実問題として、脅威ハンティングの大半は簡単な作業ではありません。調査の一環として行うものでもありません。むしろ、セキュリティ ポスチャを強化するためにあえて計画し、定期的に実施すべき業務です。セキュリティ防御策の一種であるとも言えます。

確かに、多忙な中でこれ以上の作業を増やすのは容易ではないでしょう。しかし脅威ハンティングの実施には、いくつかの大きなメリットがあります。

事前の一策

最初のメリットは、未知の脅威や未検出の脅威を特定し、根絶できる可能性のあることです。脅威ハンティングにより、たとえ脅威が特に検出されなくても、脆弱性が特定されることはよくあります。これによりセキュリティを強化し、新しいポリシーを作成できます。定期的な脅威ハンティングの実施には、攻撃対象領域を大幅に縮小できるというメリットもあります。

別のメリットは、脅威ハンティングでの学習内容に基づいて改善点を洗い出せることです。悪意のある振る舞いが発生する可能性のあるエリアに加え、脅威ハンティングを繰り返し自動実行するエリアも特定できます。そこで特定したエリアを基に追加の脅威ハンティングを実施すれば、保護機能を構築、強化することができます。

どこから始めるべきか

このホワイト ペーパーの目的は、脅威ハンティングの概要を説明することです。脅威ハンティングの詳細とその価値、参加すべき担当者、実施する内容と対象エリア、そして実施すべきタイミングについて解説します。

脅威ハンティングと内容が重なるセキュリティ分野は多数ありますが、これらの分野を比較したうえで、脅威ハンティングにセキュリティ対策としての独自の価値がある理由についても説明します。

最後に、組織内で効果的な脅威ハンティングを実施する方法を説明します。判断が難しい事柄のひとつは、どこから始めればよいかです。そのため、セキュリティを強化する脅威ハンティングポスチャの簡単な構築ステップを最初に説明します。

脅威ハンティングと他のセキュリティ業務との比較

脅威ハンティングは比較的新しいセキュリティ分野であり、他のセキュリティ業務と重なる部分もあります。脅威ハンティングに関わっている人材の多くは、他のセキュリティ業務の経験も持ち合わせています。以下は、他のセキュリティ業務との簡単な比較です。

インシデント対応

インシデント対応は、おそらく脅威ハンティングに最も似ています。どちらの分野でも、環境内の脅威に直接対処します。主な違いはインシデント対応が事後対策であることです。つまり、セキュリティアラートや、ネットワークまたはエンドポイント上での振る舞いなどの証拠を基に、ネットワーク上の「未知」や「痕跡」に対応します。一方の脅威ハンティングでは、必ずしも脅威の証拠があるとは限りません。把握している脅威を阻止や緩和するのではなく、脅威がないか能動的に探し出します。

ペネトレーション テスト

脅威ハンティングとペネトレーション テストにも類似点があります。基本的に、どちらもネットワークの脆弱性を探し出します。ただしペネトレーション テストでは一般に、ネットワークや機密情報へのアクセスを許す設定の問題や既知の脆弱性がないかを確認します。脅威ハンティングの目的は、必ずしもそれらにアクセスすることではなく、潜在的な脅威を特定して根絶し、今後の予防ポリシーを作成することです。

リスク管理

リスク管理の主な内容は、ネットワーク内またはシステム上の脆弱性を特定し、それらの重大度を判断して優先順位を決定し、必要な措置により修正することです。リスク管理では脅威の原因の特定が必要になる場合があります。脅威ハンティングがリスク評価に役立つ場合もあります。ただし一般的に、リスク評価は脅威ハンティングよりも幅広い領域を対象とし、既知と未知両方の潜在的なリスクすべてに対応します。

侵害評価

侵害評価も脅威ハンティングと同様に、ネットワークが未知の攻撃者によって侵害されていないか調べます。ただし侵害評価は、脅威ハンティングよりもはるかに広い範囲を担当します。さまざまなツールをネットワーク全体にインストールし、ネットワーク全体に異常がないかを確認します。脅威ハンティングでは、非常に具体的な想定やシナリオを基に範囲が決められ、常にそこに焦点が置かれます。

5 つの「W」

脅威ハンティングをどこから始めるかを決めるのは難しい課題ですが、ジャーナリズムでよく使用される 5 つの「W」（いつ、どこで、誰が、何を、なぜ）を利用すると、プロセスの計画をスムーズに立てられます。

脅威ハンティング チームはインシデント対応チームを兼ねる場合が多くあります。脅威ハンティングを行うことで、実際のインシデントが発生した際の対応スキルや対応時間が向上します。

理由（なぜ）

能動的な脅威ハンティングへの先行投資によって、組織のセキュリティ ポスチャを大幅に強化できる可能性があります。組織化され、優れたスキルと十分な資金を持つ攻撃者は実在しています。そうした攻撃者に狙われると、脆弱性をしらみつぶしに探して侵入される危険性があります。残念ながら、どれほど優れたセキュリティ ツールでもすべての攻撃を発見することはできません。そこで活躍するのが脅威ハンティングです。脅威ハンティングの主な目的は、脆弱性を探して侵入する攻撃者に対抗することにあります。

脅威ハンティングの他のメリットは、アウトブレイクや侵害が発生したときに役に立つツールやテクニックを練習できる点です。脅威ハンティング チームはインシデント対応チームを兼ねる場合が多くあります。脅威ハンティングを行うことで、実際のインシデントが発生した際の対応スキルや対応時間が向上します。つまり脅威ハンティングは「消火訓練」も兼ねているのです。

ユーザ（誰が）の特定

脅威ハンティング チームの設立には、さまざまな要素を考慮します。チームには、さまざまなスキル セットやバックグラウンドを持つ人々を集める必要があります。

大規模な組織であれば、グループ（タイガーチーム）が一定時間を割くだけで、脅威ハンティングを計画して実行し、報告にまで至るかもしれません。しかし専任の IT 担当者が数名の小規模組織であれば、そう簡単にはいきません。必要な人材がいなければ、外部の専門家に依頼する手もあります。ただしこれは一長一短です。長所は脅威ハンティングの経験者を利用できる点です。しかし外部の脅威ハンティング チームは社内の担当者と違い、組織のネットワークを十分に把握しているわけではありません。

どのようなケースであれ、脅威ハンティング チームに必要なコア スキルは次のとおりです。

- **エンドポイントとネットワーク セキュリティに精通している**

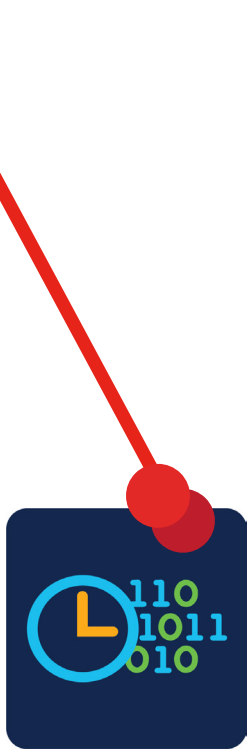
  これは言うまでもありません。セキュリティ問題やベスト プラクティスに関する幅広い知識を持つ、SOC や IT チームの経験豊富なメンバーが必要です。

- **データ分析を理解している**

  脅威ハンティングの多くの場面では、未加工のデータからパターンを見つけ出す必要に迫られます。統計分析を理解していれば、データのパターンを特定する際に役立ちます。それと同じく重要なのが、検出された異常を特定して報告するために欠かせないデータの可視化です。

- **好奇心がある**

  脅威ハンティングは単純な業務ではありません。ある意味では芸術と似ています。一見関係のない事象をつなぎ合わせたり、「こうしたらどうなるか？」と疑問を持ったりできる想像力が必要です。



実際の脅威ハンティング作業に取りかかる前に、ハンティングを実施するための適切なログ機能が有効になっていることを確認する必要があります。

セキュリティ専門家にとっての脅威ハンティングの利点は、その楽しさにあります。SOC や IT チームにとって、各自の日常業務から離れて攻勢をかけるチャンスになるからです。脅威ハンティングといった充実感のある業務により SOC 人材の定着率が上がるだけでなく、人材獲得競争が激しい分野での人材確保にも役立ちます。

ハンティングのタイミング（いつ）

最も成功するのは計画されたハンティングです。ハンティングの範囲を設定し、明確な目標を立てた上で、ハンティングに割く一定の時間を確保します。脅威ハンティングを実施した後は、セキュリティ ポスチャの改善計画を立て、セキュリティ戦略を作成することで、脅威ハンティングの結果を活かす必要があります。

脅威ハンティングを実施する別のタイミングは、疑わしい振る舞いが検出されたときです。

- **特定のユーザが通常よりもはるかに多くのデータをダウンロードしている**
- **アクセス権を持っていないシステムに、特定ユーザがログインを試みている**
- **管理者が自分の bash ログを削除した**

これらの振る舞いは、ネットワークに攻撃者が侵入した可能性を示しています。脅威ハンティングを開始すべき明確なタイミングだと言えます。

上述したタイミング以外にも、脅威ハンティングが突然行われる場合があります。たとえば、サイバーセキュリティのニュースを見た CIO が不安に駆られ、社内のセキュリティについて IT 部門に問い合わせてくるかもしれません。このような問い合わせにも対応できるプロセスを用意しておけば、時間やリソースを大幅に節約できます。

場所と内容（どこで & 何を）

脅威ハンティングの鍵を握るのはデータです。実際の脅威ハンティング作業に取りかかる前に、ハンティングを実施するための適切なログ機能が有効になっていることを確認する必要があります。システムで何が起きているのかを確認できなければ、対策すら立てられないからです。

データを取得するシステムは、ハンティングの範囲に応じて異なります。たとえば、財務部門のエンドポイントを対象にする場合もあれば、Web サーバに焦点を当てる場合もあります。環境内にツールをインストールして特定のトラフィックを監視するケースもあります。脅威ハンティングでは、これらの一時的なシステムで取得されたログが利用されます。

ただしログの収集はストレージを圧迫するほか、チームの作業時間を奪う可能性もあります。それらの事態を防ぐには、ログの保存先として物理リソースを別途確保し、ログの収集に最低限の自動化を使う必要があります。短期的には、ログの採集範囲を限定する必要があるかもしれません。ログの分析は時間を要する作業ですが、セキュリティ情報およびイベント管理（SIEM）ソフトウェアなどのツールを活用すれば時間を大幅に短縮できます。

脅威ハンティングの最初の数回は、限定範囲のログだけでは説明できない疑問も見つかることでしょう。ただし長期的には、ログの採集範囲に含めるべきシステムやレベルが判明してきます。

痛みのピラミッド

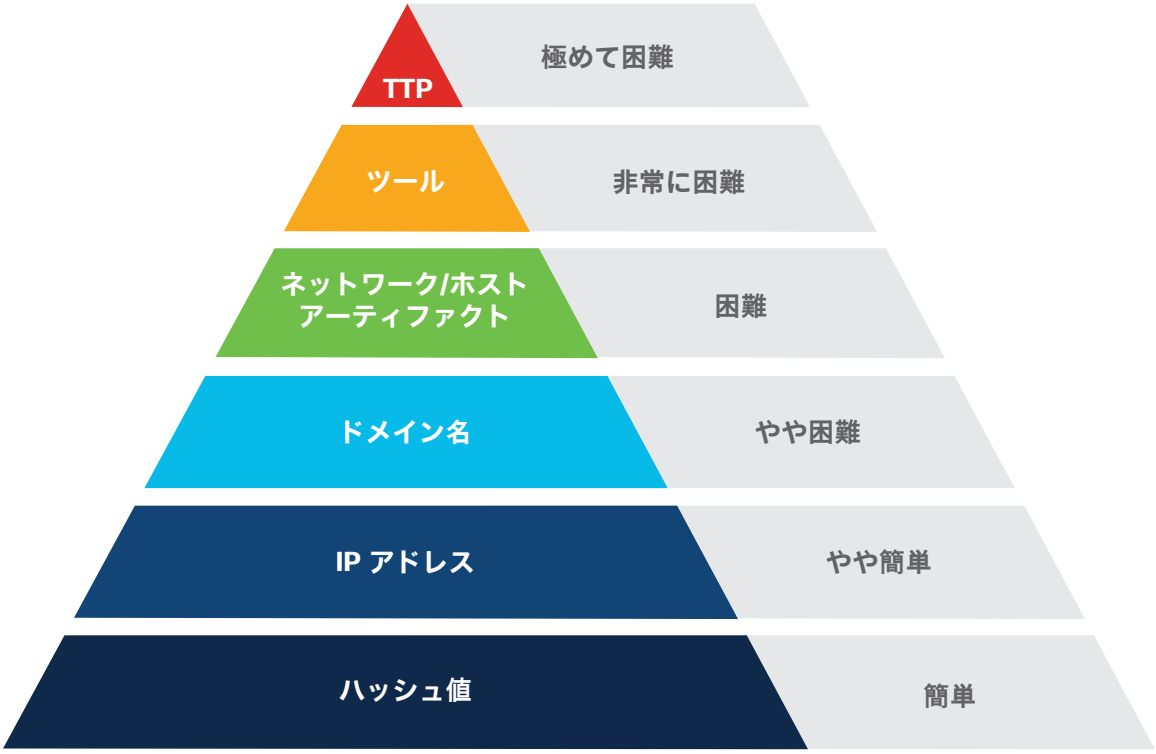
脅威ハンティングの目標は、攻撃者の TTP（戦術、技術、手順）を解明することです。これが重要な理由は、攻撃者にとって TTP を変えることが困難だからです。

セキュリティ研究者の David Blanco 氏は、ネットワーク攻撃の難易度を最大限に引き上げる「痛みのピラミッド」アプローチ（下図）を考え出しました。ピラミッドを構成する 6 つのレイヤは段階的なアプローチを表しており、難易度は上層ほど高くなります。

ピラミッドの底部は「ハッシュ」です。既知の不正ハッシュを含むファイルは簡単に検出できます。ただし攻撃者にとっても代替を見つけるのが容易です。次の層の「IP アドレス」も同様です。ただし IP アドレスの検出や代替は不正ハッシュよりも労力を要するため、ピラミッドでも「ハッシュ」より上に位置しています。次の「ドメイン」や、さらに次の「ネットワーク/ホスト アーティファクト」と「ツール」では、難易度がより上がります。

脅威ハンティングの目的はピラミッド最上層である「TTP」、つまり攻撃者の戦術、手法、手順を解明することです。これが重要な理由は、攻撃者にとって TTP を変えることが困難だからです。TTP がピラミッドのトップにある主な理由は、異なるデータ セットのデータ ポイントを比較したうえで、関係性が明らかでない事象をつなぎ合わせる必要があるからです。

ピラミッドの上層へ行くほど、ネットワークの攻撃により多くの労力を使うよう攻撃者に強いるため、攻撃の難易度を上げることができます。同時に、攻撃が検出される確率も高くなります。「痛みのピラミッド」の原則に従えば、ネットワークへの侵入を困難にし、攻撃者の狙いをより脆弱な他の組織に向けることができます。



出典：David J. Bianca 氏の個人ブログ

ハンティング方法

脅威ハンティングには、さまざまなアプローチがあります。脅威ハンティングをどの程度詳細に実施するかは、利用可能なリソースとスキルによって決まります。

次のセクションでは前半で脅威ハンティングの基礎について説明し、後半でより詳細に解説します。重要なのは、脅威ハンティングでの学習内容を積み重ねることです。必要に応じて戦略を作成し、ポリシーを変更し、自動化を実施すれば、脅威ハンティングの練度を上げるための基盤を得られます。

ログの分析

新たに発見された脅威に関する調査やレポートがきっかけとなり、荒削りの脅威ハンティングが始まることもあります。最近の脅威レポートでは、情報共有を目的として侵害の兆候（IoC）を含めるのが一般的です。IoC には、IP アドレス、URL、ドメインやファイル ハッシュといった、脅威の構成情報が含まれます。

最もシンプルな脅威ハンティングでは、IoC に照らし合わせてシステム ログをチェックします。必要なのはコマンド ライン ツールや簡単なスクリプトだけです。ただし SIEM を使用すれば、IoC とシステム ログをすばやく比較できます。SIEM よりも高度なセキュリティ製品では、IoC をコピーしてダッシュボードに貼り付けるだけで、それらが環境内にないか確認できます。

基本的な流れに慣れてきたら、次のステップに進みます。ここではログをさらに詳しく調べて、新たな IoC が潜んでいないか探します。そこで必要になるのがデータ分析スキルです。クラスタリングや頻度分布などの統計モデルを使ってログを解析し、異常を特定します。そして最終的には「痛みのピラミッド」の最上層、つまり攻撃者の TTP の特定を目指します。

実際の脅威ハンティング

Jeff Bollinger は、シスコの CSIRT チームにおけるセキュリティ調査の責任者です。自身のチームが実施した脅威ハンティングについて、以下のように述べています。

「Cisco AMP が収集したエンドポイント データから侵害の兆候を探したところ、疑わしいバイナリが意図的に削除されたことを発見しました。

そこで、お客様のバックアップ アーカイブからバイナリを復元したところ、追加の兆候である C2 のホスト名が確認されました。これらの兆候をネットワーク テレメトリ全体に適用した結果、当初のバイナリだけでは判明しなかった他の脆弱なホストも特定できたのです」

経験が豊富であっても先入観を持つことは危険です。豊富な経験は、脅威ではないことを証明するために活用してください。すぐに証明できない場合は詳しく調査しましょう。

理論のテスト

既知の IoC と照らし合わせてログを確認するだけでは十分と言えないかもしれません。その理由は、単に 1 対 1 の照合であるからです。つまり真の脅威ハンティングにはより詳しい調査が必要です。

ここでは創造性がものを言います。脅威の存在しそうな場所や、そこへの侵入経路あるいは侵入手口などを考え出す必要があるからです。以下のような調査方法が使えるかもしれません。

- **セキュリティ ニュースに目を通す**

  サイバーセキュリティの最新ニュースには、脅威ハンティングに役立つ情報が満載です。たとえば、Windows で重大な脆弱性が公開された直後であれば、関連プロセスで異常なアクティビティが発生していないか調査します。特に注目すべきは自社の業界に関連するニュースです。たとえば航空業界では（金融業界と異なり）、クレジットカード情報が盗まれたニュースの関連性はあまり高くないでしょう。逆に金融業界にとっては、航空機のソフトウェアに脆弱性が見つかっても無関係です。

- **異常な振る舞いに関するレポートを確認する**

  内部でのアクティビティに異常がないか確認します。夜間にシステムのスリープが突然解除された場合、その原因を調査します。社外に情報が漏れたとの報告が寄せられた場合、データ漏洩の兆候がないか確認します。

- **正常な状態をフィルタリングして異常を見つけ出す**

  異常なアクティビティは明確な調査対象ですが、見つけやすいとは限りません。非常に労力を要する場合もあります。

以下のような方法で、侵害の兆候となりそうなアクティビティを選り分ける必要があります。

- 長時間のネットワーク接続を探す：データ漏洩の兆候かもしれません。想定内の長時間接続を除外した上で、残りの接続について疑わしいものがないか確認します。
- CPU 使用率の上昇と、その原因となっているプロセスを探す：クリプトマイニングやトロイの木馬によるアクティビティが原因かもしれません。既知のアクティビティを除外し、それ以外のアクティビティを調べます。
- BITSAdmin ツールがダウンロードしているファイルの種類を調べる：BITSAdmin ツールは、マルウェアのダウンロードに使用される場合があります。攻撃の多くはローカル ツールを隠れ蓑として利用します。通常のダウンロード アクティビティを除外し、残りのダウンロードを調べます。
- スケジュール設定されているタスクを確認する：攻撃者は、不正なアクティビティを開始させるために独自のタスクを追加する場合があります。システム管理者以外が実行したものなど、疑わしいタスクはすべて調査してください。

異常な振る舞いを発見したら重点的に調べ、根本原因を見つけ出す必要があります。ただし慎重なアプローチも欠かせません。異常な振る舞いが必ずしも攻撃者によるとは限りません。結論を出す前に、必ず調査結果を他のデータ ソースと比較してください。また、経験が豊富であっても先入観を持つことは危険です。豊富な経験は、脅威ではないことを証明するために活用してください。すぐに証明できない場合は詳しく調査しましょう。

原因を突き止めて対策を講じる

ネットワーク内の脅威を特定した後は、侵入経路を突き止めてふさぐ必要があります。しかしその後の脅威ハンティングで、同じ攻撃者が別の方法で戻ってきたことが判明した場合、どうしますか？

常に自社が被害者となる場合は、攻撃を仕掛けている人物と、攻撃に使用されているインフラストラクチャを調査することで、攻撃者を封じる必要があります。

ただし、「ハックバック」（攻撃者への反撃）を勧めるわけではありません。ハックバックを試したくなるかもしれませんが、いくつかの問題があります。

攻撃者のインフラに反撃した場合、攻撃者がそれに気づいて「倍返し」をする可能性があります。しかも当初の目的（データの窃取など）と異なり、システムの無効化や破壊などによる復讐が目的に変わる危険性もあります。

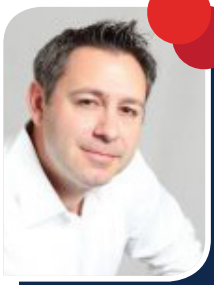
ハックバックが危険な別の理由ですが、大半の国や地域ではハックバックが法的に禁止されています。つまり、攻撃に対する「防御目的のハッキング」であっても、違法なハッキング行為だと見なされます。

ただし幸いにも、まだ多くの方法が残っています。IoC を分析すれば、反撃することなく攻撃者について多くの情報を得られるかもしれません。

攻撃者を封じる最善の防御アプローチとは、「痛みのピラミッド」の全階層であらゆる IoC を収集して攻撃者のプロファイルを作成し、警察などに提出することです。警察であれば、法的手段により攻撃者を追跡して封じることができます。

攻撃者を封じる最善のアプローチとは、あらゆる IoC を収集して攻撃者のプロファイルを作成し、警察などに提出することです。

狙われやすい大規模組織を除けば、攻撃者のプロファイルを社内で作成するとなれば荷が重いかもしれません。その場合は外部のセキュリティ調査チームに調査を委託できます（委託すべきだとも言えます）。シスコでは、Talos インテリジェンスや Incident Response サービスといった脅威インテリジェンス部門が支援を提供しています。



脅威ハンティングを活用する

シスコのセキュリティ アドバイザリ サービスの脅威管理責任者である Sean Mason は、自身のチームが脅威ハンティングを活用してきた方法について、以下のように語っています。

「脅威ハンティングの価値に気付いたのは、2011 年に起きた RSA Security 社のハッキング事件がきっかけでした。そこで、同社のような被害を防ぐための方法について話し合いを重ねた結果、別の観点から考えられるようになりました。どのような可視性のギャップがあるのかも認識できました。自身が関わったチームでは、さまざまな形でハンティングを活用してきました。推測の検証やインシデントへの対応、最新のセキュリティ ニュースを受けた調査などです。これまで 8 年以上にわたって脅威ハンティングを活用してきましたが、企業や業界を問わず、侵害を防ぐには脅威ハンティングが不可欠であると断言できます」

脅威ハンティング実施後のステップ

ネットワーク内に隠れている脅威を特定して根絶することも重要ですが、侵入経路を把握してふさぐことも重要です。これは脅威ハンティングで最も重要な部分だと言えるでしょう。そのため、結果について話し合うためのミーティングを計画してください。ミーティングでは検出結果を説明し、改善策について話し合います。ネットワーク ポリシーの変更と適応作業も必要です。

最も良いのは、脅威ハンティングで何も検出されないことです。調査した範囲にリスクがないことを確認できるからです。

検出する主眼が脅威ではなく脆弱性に置かれる場合もあります。脅威ハンティングに成功すれば、サーバの設定ミスや、修正が必要なポリシー違反などが判明する可能性もあります。ただし最も良いのは、脅威ハンティングで何も検出されないことです。調査した範囲にリスクがないことを確認できるからです。

脅威ハンティングを実施した後の別の重要なステップは自動化の追加です。脅威ハンティングが完了しても、検出された脅威が完全に消えたとは限らないため、定期的な確認が必要です。脅威ハンティングでの学習内容を活かして、繰り返し実行できるプロセスを構築します。長期的には、警報付きの「罠」を仕掛けるといったセキュリティ戦略を立てます。

まとめ

ネットワークに脅威がまったくないことを確かめる術はありません。ただし、脅威ハンティングが無意味だということにもなりません。脅威ハンティングのメリットは、侵入した脅威を根絶できることに加え、セキュリティ ポスチャを強化できることです。

脅威ハンティングとはレンガを積むようなものです。家を建てるときはレンガをモルタルで固めながら、一段ずつ積み上げていきます。そうした地道な作業も最終的には「壁」という成果になって表れます。

脅威ハンティングでも同様です。レンガの第一層は十分なログを採集することです。モルタルに相当するのは、ログを定期的に配信する自動化です。レンガの第二層はログと IoC を比較することです。これらのプロセス（レンガ）を再び自動化（モルタル）によって固めます。同時に、データ分析や理論のテストといった別のレンガも積み上げていく必要があります。

上記のようなプロセスを繰り返すことで、強力で安定した脅威ハンティング プロセスが形成され、安心感を得ることができます。

脅威ハンティングに役立つツール

脅威ハンティングに使える推奨ツールをご紹介します。これら意外にも優れたツールはたくさんありますが、脅威ハンティングを始める際の参考としてご活用ください。

Cisco Threat Response

Cisco Threat Response は、シスコのセキュリティ製品の統合を自動化します。Cisco Talos や第三者機関からの脅威インテリジェンスをセキュリティ イベントと比較することで、侵害の兆候（IoC）を自動的に探して脅威を迅速に特定します。重要な調査情報の収集と保管、進捗および結果の管理と文書化、ダッシュボードからの脅威の直接対応といった機能も提供します。

Cisco Threat Grid

Threat Grid では、高度なサンドボックスと脅威インテリジェンスが 1 つのソリューションとして統合されており、組織をマルウェアから防御します。堅牢でコンテキストリッチなマルウェア ナレッジ ベースに基づいて、マルウェアの今や今後の動作、脅威の度合い、対応策などを提示します。

Cisco Stealthwatch

Cisco Stealthwatch は包括的な可視性を提供する分析ソリューションで、ネットワーク トラフィックとクラウド セキュリティに特化しています。暗号化されたトラフィックでも、データを復号することなくマルウェアを検出できます。マルチレイヤの機械学習とエンティティ モデリングを駆使することで、高度な脅威検出、脅威対応の迅速化、ネットワーク セグメンテーションの簡素化を実現します。高度な振る舞い分析により、ネットワークまたはパブリック クラウド インフラの内部にいる人物と、その人物の振る舞いを検出できます。

Cisco Advanced Malware Protection（AMP）for Endpoints

AMP はエンドポイントを保護するだけでなく、マルウェア分析や能動的な脅威ハンティングにも貢献します。AMP の堅牢な検索機能を使えば、ファイル、ハッシュ、URL、IP アドレス、レジストリ キー、ユーザ、プロセス、アプリケーションなどの各種情報を特定できます。また、ファイルが最初に確認された日時からエンドポイントでの振る舞いに至る幅広い分析情報により、環境内でのファイルのライフサイクルも確認できます。

Umbrella Investigate

Investigate は、ドメイン、IP、自律システム（ASN）とファイル ハッシュの関係性や変化について、業界トップクラスの精細度で可視化します。Web コンソールと API からアクセスできる脅威インテリジェンスにより、脅威の検出と予測に不可欠なセキュリティ コンテキストも提供します。

セキュリティ情報およびイベント管理（SIEM）ツール

SIEM ツールは、脅威ハンティングの実施時、特に開始時に不可欠です。適切に設定された SIEM により、ログ ファイルの収集と基本分析にかかる時間を大幅に短縮できます。よく知られている SIEM には、Splunk、IBM QRadar、Exabeam などがあります。

エンドポイント モニタリング ツール

エンドポイントから詳細なログを収集するために役立つツールは数多くあります。Windows に組み込まれているイベント ログは初心者向けツールとして最適です。Sysmon や Process Monitor などの高度なツールを使用することもできます（使い始めに役立つ事前に作成された設定ファイルもあります）。Apple Mac ではコンソールでログを確認できます。

パケット アナライザ

パケット アナライザによりネットワーク トラフィックを監視できます。Wireshark や tcpdump などのアプリケーション、および pcap などの API は、ネットワークで転送されるデータについて情報を収集できる一般的なツールです。

シスコ サイバーセキュリティ シリーズについて

シスコは過去 10 年間にわたって、全世界のサイバーセキュリティ専門家を対象に、セキュリティと脅威インテリジェンスに関する多くの信頼できる情報を公開してきました。これらの包括的なレポートでは、脅威の現状や組織への影響を詳しく解説し、データ漏洩などから組織を守るためのベスト プラクティスを紹介してきました。

ソート リーダーシップに対する新しいアプローチの一環として、シスコでは一連の調査とデータに基づく出版物、『シスコ サイバーセキュリティ シリーズ』を発行しています。シリーズの分野は徐々に増え、業界や担当が異なるセキュリティ専門家に向けた幅広いレポートが登場してきました。2019 年の一連のレポートは、脅威研究者などから得られた、高度で幅広い専門知識を基に書かれています。データ プライバシー ベンチマーク調査、脅威レポート、CISO ベンチマーク調査などがすでに発行されたほか、今後もいくつかのレポートが発表される予定です。

詳しい情報や過去のレポートは、https://www.cisco.com/c/ja_jp/products/security/security-reports.html をご覧ください。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

THRT_05_0819_r1JA 19.10