Splunk Security Analytics

事例TOP5

splunk>
turn data into doing™

セキュリティイベントを迅速に検出して対応するのは簡単なことではありません。セキュリティアナリストである分析担当者は、1件のアラートの対応に何分も、場合によっては何時間も費やすことがあります。これに、アナリストが日々処理しなければならないセキュリティアラート数(数百件)を掛け合わせると、チケットが多すぎるのに対してアナリストが少なすぎることがわかります。問題が見えてきたのではないでしょうか。

発生するアラートの数を減らすとともに、セキュリティチームが対応時間を短縮できるようにすることが必要です。最初にできることは、チームが脅威をより迅速に検出して対応できるように、環境に対する可視性を向上させることです。さらに、アラートのトリアージに自動的に対応すれば、数分かかっていた時間を数秒に、また数時間を数分に短縮することができます。これを望まない人がいるでしょうか。

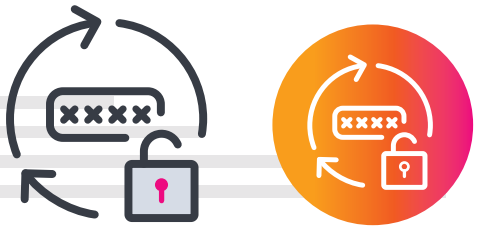
これにより、マルウェアのような検出が困難で巧妙な脅威が隠れたり拡散したりする場所を減らし、脅威がもたらす損害額を減らすことができます。ストレスのたまったセキュリティアナリストも楽になります。

ただ、アナリストが楽になるとは言っても、急速に変化するセキュリティの世界で生き抜くのは必ずしも簡単ではなく、セキュリティチームは引き続き、セキュリティの取り組みにどこから着手するか考え出さなければなりません。そして、すでに立証されているように、組織内のあらゆる箇所に不正侵入のおそれがあり、時間的余裕をもってセキュリティギャップを特定する必要があることを考えると、その対応は、最高レベルのアナリストにとってさえ非常に困難な仕事となる可能性があります。

ここで、すべてのセキュリティアナリストにとって朗報があります。Splunkでは長年にわたり、お客様と一緒にまさにこの問題に対処する方法に取り組んできました。セキュリティに関する非常に難しい問題についても、お客様のデータの内部に隠された答えを解き明かすことでお客様を支援してきました。

セキュリティのユースケースの概要と着手の方法を示したこのクイックガイドには、こうしたお客様との対話がまとめられています。どれも、よく質問を受けるセキュリティの問題です。さらに、コンテンツのベストプラクティスや、Splunk Enterprise Security (ES)の導入や改良にあたってセキュリティチームがすぐに全力を発揮できるようにするためのアイデアも記載されています。

01



認証情報への侵害

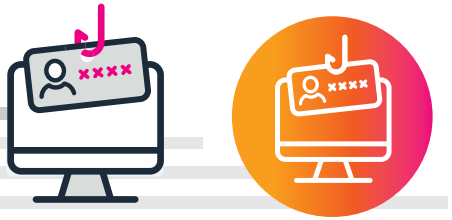
ユーザー認証情報の侵害とは?

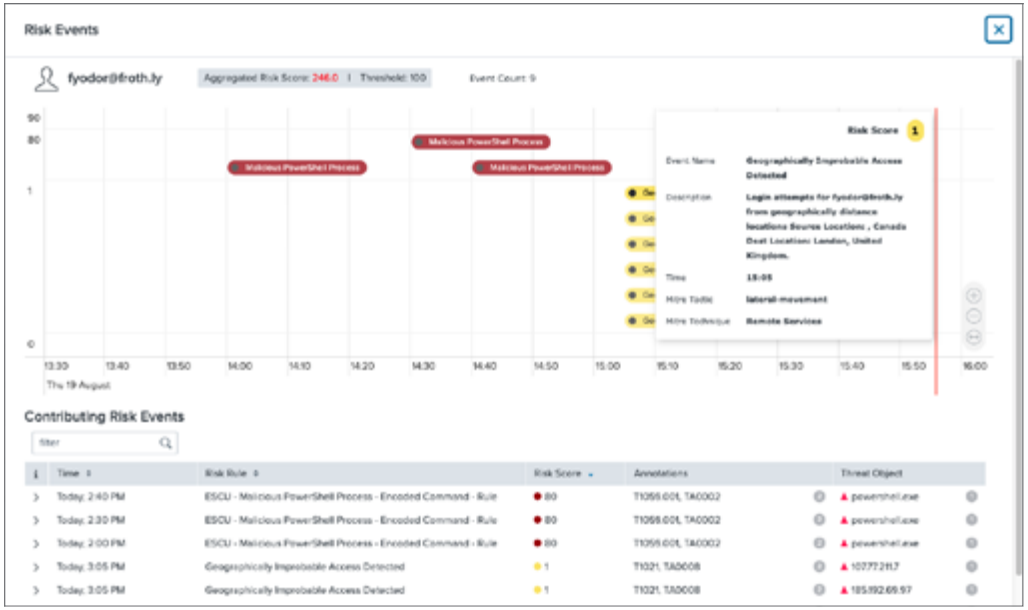
ユーザー認証情報の侵害とは、実証済みの手法(フィッシング攻撃やビジネスメールの悪用など)を用いて攻撃者が従業員の認証情報を入手することを指します。攻撃者は、有効なユーザー認証情報を使用して環境に侵入すると、目的を達成する(そしてセキュリティアナリストの1日を台無しにする)ための脆弱性を探し始めます。最悪なのは、攻撃者が有効な認証情報を使用してログインしているために、完全に正当なユーザーのように見えることであり、それがこの脅威の検出を困難にしています。

ユーザー認証情報の侵害にSplunkはどう対処するのか?

Splunk Security Analytics (SSA)は、ユーザー認証情報が侵害され、認定ユーザーまたは認定アプリケーション以外の誰かが使用しているインスタンスを特定できます。SSAは共有および汎用のアカウントの使用にも対応しています。SSAの行動モデリングでは、通常の行動として定義された行動とは異なるアクティビティをユーザーが実行すると、アナリストに通知が送られます。検出の範囲には、Active Directory (AD)の通常とは異なる、または悪質なアクティビティ(自身に対する操作、終了したユーザー、無効になったアカウント、アカウントの復元など)の特定が含まれます。

02





Splunk UBAを使用すると、通常の行動をベースラインとして用いて、リスクの重大度のスコアを算出できます。

特権ユーザーの侵害

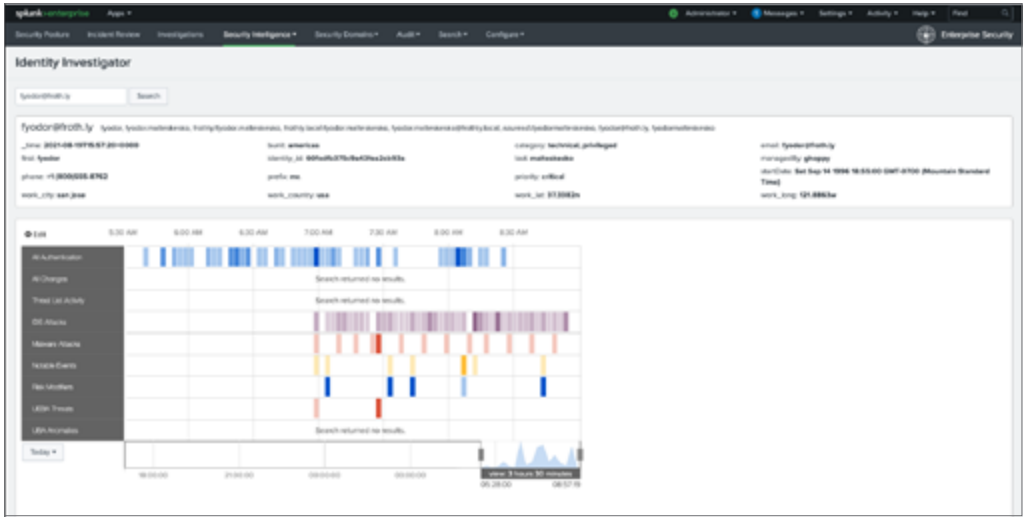
特権ユーザーの侵害とは?

特権ユーザーの侵害とは、ソーシャルエンジニアリングの手法やゼロデイエクスプロイトにより、ハッカーが特権ユーザーアカウントへのアクセス権を取得することを指します。通常、このような攻撃でハッカーが標的とするのは、機密性の高い資産への管理者アクセス権や経営幹部レベルの権限を持つ優先度の高いユーザーです。このため、特権アカウントの侵害が発生したときは、セキュリティアナリストが直ちに特定することが重要です。実際の手法では、ハッカーは通常、既知の脅威を防御するために構築されたファイアウォールや従来のSIEM (Security Information and Event Management)ソリューションなどの従来型セキュリティツールをすり抜けます。一度侵入してしまえば、パスワードやSSH鍵などの機密情報を集めて、さらにアクセスする方法を探り始めます。

特権ユーザーの侵害にSplunkはどう対処するのか?

Splunk Security Analytics (SSA)は、各アカウントの行動のベースラインを作成し、ユーザーのベースライン行動と比較して異常を特定します。これにより通常、過度の使用、まれなアクセス、妨害の可能性、痕跡の隠ぺいが明らかになります。ユーザーが、既知の通常の行動とは異なる行動を続けると、SSAの確度が上がり、リスクの可能性と重大度が高まります。たとえば、サービスアカウントを使用したVPNアクセスや対話型ログイン、データの不正閲覧、監査ログの削除、機密情報へのアクセスなどを検出できます。

03



内部脅威の特定に役立つSplunkダッシュボードの一例。

内部脅威

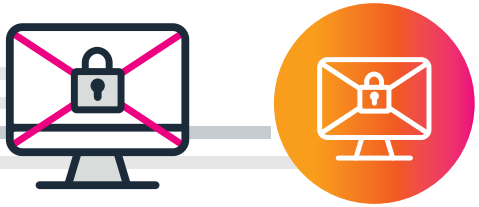
内部脅威とは?

内部脅威とは、機密情報に意図的に、または誤ってアクセスできる従業員や業務を委託した業者が、そのアクセス権を誤用して、勤務先の企業に被害を与えることを指します。内部脅威は、攻撃やデータ損失の3分の2を占めるほど一般的な問題です。ユーザー認証情報の侵害、特権ユーザーの侵害、内部脅威はどれも、有効な資格情報が不正な理由で悪用されるという行動に関連するものです。

内部脅威にSplunkはどう対処するのか?

Splunk Security Analyticsは、攻撃者が社内、クラウド、モバイルの環境を動き回った痕跡を捕捉します。このようなアクティビティは高度な機械学習アルゴリズムにより分析され、ベースラインの作成、逸脱の検出、異常の発見がほぼリアルタイムで行われます。環境内でのハッカーの行動全体がわかりやすいシーケンスとしてつなぎ合わされ、パターン検出と高度な相関付けを駆使してキルチェーンを明らかにすることができるため、セキュリティチームは迅速な対応を取ることができます。

04



ランサムウェア

ランサムウェアとは?

ランサムウェアはマルウェアの一種で、残念なことにますます増えています。この脅威は、バイデン大統領の関心すら引いています。この攻撃ではまず、ハッカーがフィッシング攻撃を用いて、疑いを持たないユーザーに特権アクセスを提供させます。続いてマルウェアが素早く行動に移り、ユーザーの一部(またはすべて)のファイルを暗号化します。攻撃者はさらに、ファイルのロックを解除する見返りとして、暗号通貨で数万ドル(場合によっては数百万ドル)に及ぶ身代金(これが攻撃名の由来)を要求します。

ランサムウェアにSplunkはどう対処するのか?

Splunk Security Analyticsは、Splunk ES Content Update (ESCU)から更新を受け取ります。ESCUは、進行中の急を要する脅威、攻撃手法、その他のセキュリティの問題にセキュリティアナリストが対処するのに役立つ事前パッケージ済みセキュリティコンテンツを提供します。現時点で、ESCUではランサムウェアのユースケースが35個提供されています。新しい脅威が特定されると、Splunkのセキュリティ脅威インテリジェンスチームがリバースエンジニアリングして、ESCUから更新がプッシュされるため、常に最新の脅威に対応できます。

05

クラウドセキュリティ

クラウドセキュリティとは?

クラウドセキュリティは、「サイバーセキュリティでは境界という考えを脱却し、ネットワーク中心のアプローチに終止符を打つべきである」という原則に基づいています。コロナウイルス感染症のお陰で、在宅勤務が増えて、クラウドへの大規模な移行が実現しました。

クラウドコンピューティングが台頭し、Google Cloud Platform (GCP)、アマゾン ウェブ サービス (AWS)、Microsoft Azureなどのパブリッククラウドにビジネスの重要な部分を移行する企業はますます増えています。このため、企業がデータをリアルタイムで簡単に分析し、ハッカーより一歩先を行くために可視性を向上させることが重要です。

クラウドセキュリティの対応範囲をSplunkはどう拡大しているのか?

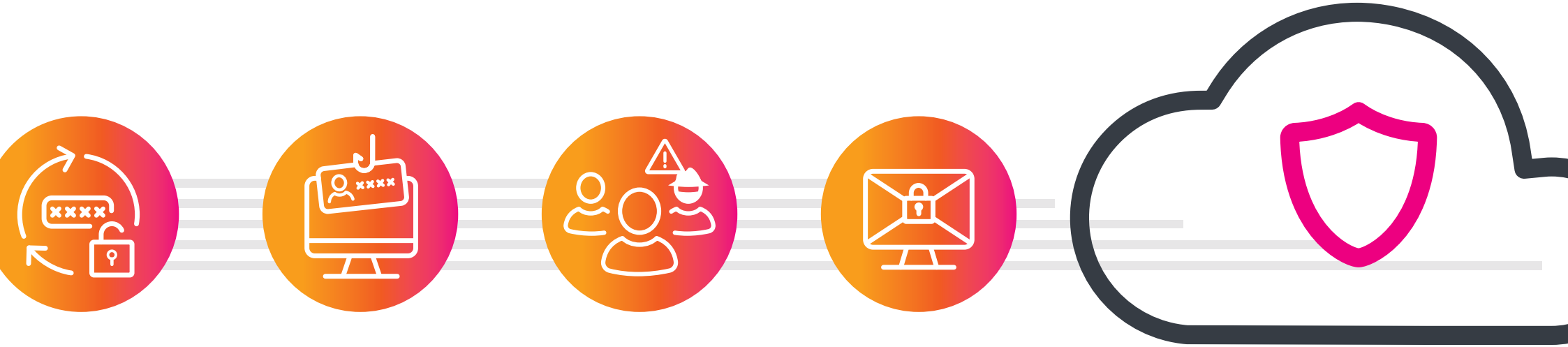
Splunk Security Analyticsにより、GCP、AWS、Azureの資産とID (A&I) 情報を簡単に取り込んで、Splunk内のA&Iテーブルにシームレスに追加できます。SSAはまた、認証、ネットワークトラフィック、構成の変更に対応するため、3大クラウドプロバイダー向けのすぐに使える検出も提供しています。前述のクラウドプロバイダーのデータモデルをSplunkの共通情報モデル(CIM)にマッピングすることで、企業の既存の検出と調査のワークフローに、クラウドデータという極めて重要な対応範囲が組み込まれます。

クラウドベースの分析主導型
SIEMソリューションを活用して、

侵害を阻止しましょう。

Splunkを始める方法をご確認ください。

詳細はこちら



21-20968-Splunk-Top 5 Use Cases for Splunk Security Analytics-LS-JA-202201