Splunk SOC：Splunk Attack AnalyzerとSplunk SOARでフィッシング攻撃のMTTDを7分に短縮

主な課題

SplunkのSOCアナリストに届くフィッシングのアラートは1カ月で数百件にも上り、その対応による負担が増大していました。また、MTTRが長く、1カ月に実行できる詳細な調査の回数が減っていました。

主な成果

Splunk Attack Analyzerを導入したことで、インシデント対応チームは調査時により多くのコンテキストを得て、脅威をすばやく封じ込めることができるようになりました。その結果、フィッシングアラートの解決時間を90%短縮できました。

業種：テクノロジー

ソリューション：セキュリティ

製品：Splunk SOAR、Splunk Attack Analyzer

フィッシングを逃さず捕らえる

フィッシングは、件数においても被害額の大きさにおいても突出している攻撃ベクトルの1つです。Splunkの『2024年セキュリティの現状』レポートでは、調査対象となった組織の88%が、生成AIの普及によって今後フィッシングの件数がさらに増え、成功率が高まると懸念しています。Splunkの社員は、不審なメールを受け取った場合、組織の安全を守るためにSplunkの検出/対応チームに報告することになっており、チームのもとには毎月数百件のアラートが届きます。多くは誤報ですが、中には実際にリスクをもたらすものもあります。いずれにしても、アナリストは詳しい調査を行って、リスクの有無を判断する必要があります。

大量のアラートを効率的に処理するために、SplunkチームはSplunk SOARを導入することを決めました。メールアラートが届くと、Splunk SOARが自動的にチケットを作成し、情報を抽出します。この方法は改善の第一歩としては効果的でしたが、Splunkの検出/対応チームはさらにMTTD (平均検出時間)を7分以下に短縮したいと考えていました。そのためには、アラート対応プロセスの中の調査の部分も自動化する必要があります。こうして、Splunk Attack Analyzerも導入することが決まりました。

成果

- フィッシングアラートの解決時間を90%短縮
- フィッシングの検出精度を向上
- サイバーセキュリティ脅威への対応と封じ込めを迅速化

以前は、フィッシングの報告が大量に寄せられ、チームによるトリアージが間に合わず、チケットのバックログがたまっていましたが、Attack Analyzerの導入後は、チケットの調査と解決にかかる時間を90%短縮することができました。フィッシングの可能性がある不審なメールが報告されると、SOARがチケットをオープンすると同時に、そのメールは分析のために自動的にAttack Analyzerに送られます。Attack Analyzerは、攻撃チェーン全体を調査してから、受け取ったメールごとに、脅威の重大度を示すスコアと判定を割り出します。その後、分析結果と関連フォレンジックをチケットにアップロードします。これらすべての処理が数分で完了するため、アナリストは以前よりも簡単に脅威の対応と封じ込めを行えるようになりました。その結果、脅威の対応と封じ込めにかかる時間が大幅に短縮され、フィッシングによる侵害やダウンタイム発生のリスクが軽減されました。

難易度の高いインシデントに対処

インシデント対応での判断は常に適切であるべきです。それはどのような組織のサイバーセキュリティチームでも同じですが、組織で発生した重大で難易度の高いインシデントに対応するSplunk Advanced Threat Responseチームにとってはなおさらです。このチームは10人のメンバーで構成され、SOCやその他の社内ステークホルダーと協力してSplunkのセキュリティを維持しています。何か問題が発生したときは、組織の運営、財務、評判への影響を最小限に抑え、全社員が最高のパフォーマンスを発揮して仕事を続けられるようにすることがチームの任務です。

チームは先日、インシデント調査をより詳細に行い、多くの分析に対応できるようにするために、Splunk Attack Analyzerを導入しました。それ以来、このツールは不審なファイルやドメインの分析に欠かせない存在になりました。Splunk Attack Analyzerを活用することで、チームはインシデントをより迅速に検出し、組織へのリスクを軽減できるようになりました。「特に難易度の高いインシデントの解決に役立っています」と、Splunk Advanced Responseチームのシニアマネージャーであるトニー・イアコベリ（Tony Iacobelli）は評価します。

> チームメンバー全員がAttack Analyzerを好んで使用しています。そういうツールはめったにありません。限界まで処理を任せても成果を出してくれることを全員が認めています。また、不可解で漠然とした未知の問題に直面しても、Attack Analyzerが真っ先に霧を晴らして状況を明確にしてくれます。
>
> Splunk Advanced Response
> シニアマネージャー、**Tony Iacobelli**

Splunk Attack Analyzerのような強力な自動脅威分析ツールがあれば、検出範囲を拡大することもできます。以前は、何らかの脅威が発生した場合、Advanced Threat Responseチームは、EDRソリューションが自動的に脅威をブロックして、さらなる攻撃を食い止めるのを期待するしかありませんでした。現在では、Attack Analyzerのおかげで、アナリストがパターンを追跡し、IoC (侵害の兆候)やホストベースのアーティファクトなどの攻撃元に関する詳細を収集して、EDRで見逃された可能性のある不審なアクティビティがないか確認できます。また、インタラクティブなデトネーションモードを使って、ツール内で安全にマルウェアを実行し、マシンへの感染リスクを負うことなく調査を行うこともできます。

ツールの追加は良いタイミングで行われました。「当時は、ユースケースの数を増やし、可視化の範囲を拡大している最中でした。しかし残念ながら、システムの可視化は進んでも、人的リソースは簡単に増やせません。そのため、チーム全体の効率を向上させて生産性を高める必要がありました。そこで活躍したのがAttack Analyzerです」とTony Iacobelliは説明します。Attack AnalyzerによってSplunkのインシデント対応チーム全体の効率が向上したことで、重大なユースケースでMTTDを7分以下に抑えるという目標を達成できました。

splunk>

お問い合わせはこちら：https://www.splunk.com/ja_jp/talk-to-sales.html
〒100-0004 千代田区大手町1-1-1 大手町パークビルディング 8階

www.splunk.com/ja_jp
splunkjp@splunk.com

24-643263-Splunk-SOC-CS-JA-202410