Splunkのセキュリティチームが明かす、顧客と自社環境を保護するための取り組み

主な課題

Splunkにとって、自社とお客様を保護することは最優先事項であり、当社のセキュリティチームは、絶えず進化するサイバー脅威の状況に先手を打つために、俊敏性、柔軟性、レジリエンスを備えている必要があります。

主な成果

SOCの中核にSplunkプラットフォームを据えることで、チームは脅威に立ち向かい、複雑な環境を保護し、お客様がセキュリティを強化するのに役立つツールを提供するために必要な可視性とインサイトを得ることができました。

業種：テクノロジー

ソリューション：セキュリティ、プラットフォーム

Splunkはその経験から、お客様が直面するセキュリティ上の課題を熟知している

ますます巧妙化するサイバー脅威は、7,500人のSplunk社員にとって絶え間ない脅威となっています。分散データが増加することで、エンドツーエンドでのセキュリティの確保はこれまで以上に困難を極め、クラウドトランスフォーメーションによって攻撃対象領域も拡大しています。

Splunkは、世界規模で高成長を遂げている企業であり、お客様と同様に、こうしたさまざまな課題に直面してきました。しかし、複雑な環境を詳細に可視化するSplunkプラットフォームを使用することで、セキュリティチームはこれらの課題に対してレジリエンスを維持し、脅威に立ち向かい、顧客を保護し、システムとSplunk社員のセキュリティを常に確保しています。Splunkプラットフォームがあれば、セキュリティ、IT、DevOpsの各チームが共通認識を持ち、グローバルなインフラを包括的に可視化し、絶え間ない脅威に直面する環境でもレジリエンスを維持できます。

データ活用の成果

30%
セキュリティのユースケース全体におけるMTTRの平均短縮率

市場初
Log4Shellに関する規範的なガイダンスを発行

向上
分散したエコシステム全体の可視性

真の脅威とノイズ(無関係な情報)を切り離す

Splunkの脅威対策チームは、セキュリティイベントが通知されたら直ちに対応できるよう準備し、万全なセキュリティ態勢を取るために迅速に作業に当たる任務を負っています。しかし、毎週何百ものアラートが生成される環境では、対応が必要な真の脅威とノイズを切り分けるのは至難の業です。

当社のチームは、Splunk SOARで手作業を削減して脅威への対応方法を最適化し、その過程で生じるコストも抑えています。チームメンバーは、プレイブックを活用してサーチを繰り返し実行したり、ワークフローを自動的に強化したりすることで、時間のかかる反復作業ではなく重要な戦略的プロジェクトに集中できます。Splunkで監視運用担当シニアマネージャーを務めるMatthew Bellezzaは、次のように述べます。「Splunk SOARのプレイブックを使えば、詳細をサーチに付加する作業がすべて自動化されるため、アナリストが追加情報を探し回ったり、別のコンソールに移動したりする必要がありません。そのため、ビジネスが拡大しても、SOCをとても効率的に低コストで運用できます」

Splunkではこうした作業を効率化することで、すべてのユースケースでインシデントのMTTRを30%短縮し、単一のユースケースでもMTTRを84%改善することができました。「分析の速さと綿密さに関してSplunkの右に出るソリューションはありません。ですから、真っ先にセキュリティチームの目にとまるのがSplunkです」と、検出エンジニアリング担当シニアマネージャーのJonathan Heckingerは述べます。「私がSplunkの顧客だった頃もそうでしたが、現在もSplunk SOCが顧客とSplunk社員を保護し続けています」

> 分析の速さと綿密さに関してSplunkの右に出るソリューションはありません。ですから、真っ先にセキュリティチームの目にとまるのがSplunkです。私がSplunkの顧客だった頃もそうでしたが、現在もSplunk SOCが顧客とSplunk社員を保護し続けています”
>
> **Jonathan Heckinger**、Splunkの検出エンジニアリング担当シニアマネージャー

Log4Shellの発見

セキュリティ対策に終わりはありません。Splunkは、30億ドル規模のビジネス、および顧客の組織を脅威の絶え間ない攻撃から保護するために、24時間365日のセキュリティ態勢を敷いています。2021年の後半には、Log4Shellが発見され大きな話題となりました。広く使用されているJavaのログ出力ライブラリに見つかったこのゼロデイ脆弱性が悪用されると、攻撃を検出されることなくリモートコード実行攻撃を行えるようになり、世界中の数え切れないほどのアプリケーションが重大な脅威にさらされることになります。Splunkは自社でその脆弱性を修復するだけでなく、すぐに本格的な対応に入りお客様にも同じ修復手順をお伝えしました。

Splunkのセキュリティ脅威調査チームは、Splunk Enterprise Securityを使用して、約12時間で潜在的に脆弱なアセットを迅速に隔離し、インシデント対応手順を開始して脆弱性を緩和しました。チームはLog4Shellに関する重要なメッセージを共有することに決め、顧客のみならず一般ユーザーも対象に、市場初の対応プレイブックを開発したのです。これにより、サイバーセキュリティおよびインフラストラクチャセキュリティ庁(CISA)は、SplunkをLog4Shellに関する規範的なガイダンスを発行した最初のサイバーセキュリティ企業として認定しました(厳密には、13件の検出報告と9件のプレイブックを発行)。

データに依存しないSplunkプラットフォームを活用すれば、重要な場面で十分な情報に基づいて的確な意思決定を行うことはもちろん、迅速に行動して顧客をサポートし、メディアの見出しを飾るような脅威から顧客を守るためのツールを提供するという、Splunkの価値を実現できます。

お客様、そして私たち自身への約束を果たす

Splunkは、自社のテクノロジーと、Splunk社員やお客様からなる素晴らしいコミュニティのおかげで、この10年間で15件の買収を含め、大規模で歴史的な成長を遂げてきました。これにクラウドトランスフォーメーションへの取り組みも加えて構築された複雑なテクノロジーエコシステムを、どんな時もその隅々まで厳重に保護するよう努めています。130カ国以上のお客様に安全な環境を提供するために、当社ではSplunk Cloud Platformを使用して、お客様のビジネスをはじめ、当社のビジネスにも影響を与える可能性のあるセキュリティの対象範囲内にあるギャップを可視化し、積極的に解消しています。

Splunk Cloud Platformを使用することで、検出エンジニアリングチームは、環境全体におけるエンドツーエンドの可視性の測定、不足しているデータや不完全なデータの確認、セキュリティ態勢を継続的に改善するための経営陣との連携が行えます。これが、どんな新たな脅威が出現しようとも、Splunkとお客様がレジリエンスを維持していくための鍵となるのです。

Splunkの無料トライアルをダウンロード、またはSplunk Cloudの無料トライアルをお試しください。Splunkは、クラウドかオンプレミスか、また組織の規模の大小などにかかわりなく、お客様のニーズに最適な展開モデルでご利用いただけます。

splunk>

営業への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

© 2023 Splunk Inc. 無断複写・転載を禁じます。Splunk, Splunk>およびTurn Data Into Doingは、米国およびその他の国におけるSplunk Inc.の商標または登録商標です。
他のすべてのブランド名、製品名、もしくは商標は、それぞれの所有者に帰属します。

23-71455-Splunk on Splunk for Security-CS-SS-JA-202305