DATASHEET

proofpoint

PROOFPOINT THREAT RESPONSE

完全な情報漏洩に至らないようにセキュリティアラートとインシデントを予防

Proofpoint Threat Responseは、セキュリティアラートが起きた際に、豊富なコンテキストデータを適用してインシデントレスポンスを自動化します。この業界初の脅威マネジメントプラットフォームは、すぐに活用できる(actionableな)インテリジェンスを生成し、システムへの感染を確認し、セキュリティ対策を自動または手動で適用する事ができます。

セキュリティイベントのコンテキスト、フォレンジック及びインテリジェンスを収集/解析することにより、自動または手動の対策を生成します。このプラットフォームは、検知と防御の間にあった隙間を埋めることにより、脅威を封じ込め、感染が広がるのを防ぎます。

Threat Responseのメリット

- 疑わしいシステムからのフォレンジックデータを自動的に収集し、時間を節約します。
- PCのデータとフォレンジックを照合することで、時間のかかる感染確認作業を短縮します。
- 外部のデバイスや外部のインテリジェンスソースからの手作業によるデータ収集を減らすことができます。
- インシデントと脅威処理をビジュアルに表示します。
- 一貫した解析が一貫した対策を可能にします。
- 統合ビューにより、意志決定を加速します。
- 自動または手動による隔離と封じ込めで、迅速な防御を実現します。
- 適用デバイス上のユーザー、ホスト、IP、URLのライフサイクル管理を自動化します。
- 対応アクションの簡易的な監査証跡により、既存インフラのROIを向上させます。
- カスタムソフトウェアモジュールへの依存を削減します。
- 自動インシデント生成とインシデント追跡管理機能により、手作業での入力を削減します。
- 狙われたユーザー、システム、グループ、部門についてのレポートをリアルタイムに提供します。

手作業での対応では追いつかない

多くの組織において、セキュリティインシデントへのレスポンスは人手に頼った時間のかかるプロセスで、そのとき稼働している人員によっては、レスポンス終了までに数日から数週間を要することもあります。このような時間のかかるタスクは、重大なボトルネックとなりますが、それを省略することはできません:

- 高い攻撃価値を持つ標的を特定し、脅威を優先度づけします。
- 大規模攻撃の一部またはボットネットによるものと考えられる脅威を特定します。
- 感染の兆候を検知するために、エンドポイントのフォレンジックを収集してレビューします。
- 対策を適用するために、時間のかかるセキュリティチームとインフラチームの間の調整を行います。

インシデント毎にこれらのタスクを全て行っていては、セキュリティチームが1日中働いても追いつきません。その結果、特定のステップを省略したり、簡易化したりすることになります。

インシデントレスポンスのための調査には時間がかかる

インシデントレスポンスのための調査には、複数の独立したソースからの情報を収集し、それらを再構成して解析しなければなりません。同時に、侵害された1台または複数のシステムを手作業で確認する必要もあります。調査に時間をかけている間に大切なデータが盗み出されたり、攻撃者がネットワーク内を移動してしまうこともあるため、完璧な調査を目指すことがさらなるリスクを呼び込むことになりかねません。

Threat Responseによってインシデントレスポンスを加速

手作業による脅威ソースの収集と調査

インシデントレスポンスには、4つの主要な目標があります:

1. 標的となったユーザーとシステムを含む、Who/What/Whereの調査。
2. 標的となったシステムのフォレンジックとサンドボックスフォレンジックレポートの検証。
3. 隔離と封じ込めにより、情報や知的所有権の流出を防止。
4. インシデントレスポンスのKPIを追跡し、インシデントを見逃したり、忘れられたり、残されたりすることを回避。

これらの目標により、どのユーザーが感染したかや脅威の深刻度と緊急度を特定し、フォルスポジティブを排除し、感染の広がりを抑え、データの流出を防ぐことができます。

Threat ResponseによるWho/What/Whereの特定

ネットワーク上のどのユーザー、部門、グループが影響を受けたかを即座に特定できます。「Who」を知ることにより、高い攻撃価値を持つCFOや幹部社員、ファイナンスシステムなどが標的となった場合には、高い優先度を付与することができます。

内部のコンテキストとインテリジェンスに加え、外部の因子もまた、セキュリティアラート内の疑わしいIPやドメインに関する手掛かりを与えてくれます。これらの因子はあらかじめThreat Responseに組込まれており、セキュリティチームのための自動解析に活用されます。

いくつかの主要な外部因子は以下の通りです:

- ドメインの新しさ/最近の登録かどうか。
- ドメインブラックリスト。
- IP及びURLのレピュテーション。
- IPジオロケーション。

自動的なIOC検証による感染の確認

Threat Responseは、標的となったシステムからエンドポイントのフォレンジックデータを収集し、Indicators of Compromise (脅威の痕跡、IOC)のスナップショットを生成します。IOCデータにはシステムの最近の変更 (レジストリと修正されたファイル) のリスト、アクティブなプロセス、ネットワーク接続などが含まれます。この情報はマルウェア解析システムやその他のシステムからのイベントと比較され、クライアントの健康状態を示す指標を提供します。

その他の重要な機能には、攻撃されたシステムの過去の感染についてのチェックがあります。Threat Responseがオンデマンドでエンドポイントからの情報収集を行う際に、現在の攻撃についてのIOCだけでなく、Threat Responseがそのサイトで観測した過去の感染に関するIOCもチェックします。これにより、過去の攻撃が永続化しておらず、標的システムから外部に拡散していないことを迅速かつ効果的に確認できます。

Premium Intellience及びサードパーティツールとの統合

Threat ResponseとVirusTotalはあらかじめ統合されており、ファイルは一度だけで無く何度もチェックされます。ダウンロードや解凍など、感染が疑われる場合には50以上のアンチウイルスエンジンによりマリシャスなシグネチャや特性がチェックされます。

Threat Responseに組込まれたPremium intelligenceからのデータを使って、各々のセキュリティアラート及びサンドボックスレポートで提供されるドメインとIPを自動的にチェックします。不正サイトを見極めるためには、攻撃IPやホストについての情報を得る必要があり、そのために外部のインテリジェンスサービスにアクセスして個別に検索していました。その作業を人手により何時間もかけて行っていましたが、自動化によってその必要は無くなりました。

この解析により、すぐに活用できるインテリジェンスを得ることができるようになり、Threat Responseが実行すべきアクションの優先度づけが可能になります。

脅威の封じ込め

情報の流出を止めるため、ネットワークレベルの変更を即座に保護に反映させます:

- ひとつのシステムから他に広がらないよう、感染を止める。
- マルウェアにコントロールシグナルが到達するのを遮断する。
- 重要情報が外部に流出することを防止。

Threat Responseは、既存のデバイスを使った封じ込めを自動化し、脅威の検知と保護の隙間をリアルタイムに埋めることができます。

「Proofpointは、私達のチームにインシデント毎の詳細なコンテキストデータを提供してくれ、検知と対策の間にあった隙間を埋めてくれました。また、ネットワーク適用オプションにも様々なものが用意されています。まるで私達のためのインシデントレスポンスアナリストを採用したようなものです。」

Kevin Moore, Director of Information Technology at Fenwick & West, LLP

スペック

イベントソース

- Proofpoint Targeted Attack Protection
- FireEye MPS
- Palo Alto Networks WildFire
- HP ArcSight
- QRadar/Juniper STRM
- Splunk
- Cisco FirePOWER NGIPS
- Suricata

適用デバイス

- Cisco ASA
- Palo Alto Networks
- Check Point
- Cisco IOS
- Juniper SRX (JUNOS)
- Fortinet FortiGate
- Blue Coat
- Microsoft Exchange/O365
- OpenDNS

Proofpointについて

Proofpoint Inc. (NASDAQ:PFPT) は、人々の働き方を守るクラウドベースのソリューションを提供する、次世代をリードするセキュリティ企業です。Proofpointはサイバーセキュリティのプロフェッショナルを助けてメールやソーシャルメディア、モバイルアプリなどを介して配信される先進的攻撃からユーザーを守り、ユーザーが産み出した情報を攻撃やコンプライアンス上のリスクから守り、問題が起きた場合には迅速に対処できるように適切なインテリジェンスとツールを提供します。フォーチュン100企業の半数以上を含むあらゆる規模の組織がProofpointのソリューションを採用しており、現代のモバイル/ソーシャルに対応したIT環境を守り、クラウド及びビッグデータ解析プラットフォームを活用して先進的脅威と戦っています。