AKAMAI 製品概要

巧妙に隠れた脅威も検知する Akamai Hunt

脅威とリスクを検知、緩和するセキュリティサービス

Akamai Guardicore Segmentation のインフラと Akamai の大規模なグローバル脅威インテリジェンスを活用し、ネットワークに隠れた巧妙な脅威を阻止

最新の攻撃は、恒常的にセキュリティ制御を回避

侵害はいつどのような環境でも起こりうるという認識のもと、最先端のセキュリティソリューションさえも常に回避する異常な攻撃性ふるまいや巧妙な脅威を、Hunt チームは常時探索しています。ラテラルムーブメント（横方向の移動）、マルウェアの実行、キルチェーンにおける早期段階におけるコマンド & コントロールとの通信などの手口を検知すれば、仮にセキュリティ制御が失敗した場合でも、大惨事を回避することが可能です。Hunt を導入すれば、ネットワークで検知された重大なインシデントがただちに通知されます。さらに Akamai のエキスパートがチームとの緊密な連携のもと、侵害されたアセットを修復し、迅速に対応します。

Hunt のプロセス

収集	分析	調査	アラート	緩和
Hunt が幅広い発信源から**一意の信号を収集**	プラットフォームが各種検知アルゴリズムを使用して**このデータを分析**	エキスパートが**疑わしいイベントを調査**し、誤検知を最小限に抑制	プラットフォームが脅威に関する**詳細なアラート**と対策の手順を送信	Hunt チームが**脅威緩和**プロセスで支援

主な機能

エキスパートの人間による 24 時間体制の分析

当社のサイバーセキュリティのプロフェッショナルは、セキュリティリサーチ、攻撃的なセキュリティ、軍事インテリジェンス、レッドチーム、インシデント対応、データサイエンスなど、幅広いフィールドから招集されています。

実際の脅威に限定したアラート

アラート疲れを防ぐため、Hunt チームは、お客様に送信するアラートを真の脅威のみに限定することでフォールス・ポジティブ（誤検知）を確実に回避します。当社のエキスパートは、グローバルな顧客基盤から収集したデータを駆使して、データセンターとクラウドアプリケーションの通信の「健全」基準を維持します。これにより、最も影響の大きい脅威を検知できます。

独自のハンティングツール

Hunt のエキスパートは、ユーザーおよびネットワークアクティビティの異常なふるまい、実行可能な分析、ログ分析など、高度な脅威ハンティングアルゴリズムを定期的に開発し、迅速な検知と対応を実現する強力なツールセットを構築します。エンドポイントとサーバーにリアルタイムでクエリーを送信するパワフルな osquery ベースツールの Akamai Guardicore Insight が、追加コストなしでサービスに含まれています。

ビジネス上のメリット

現在進行中の攻撃を検知
Hunt チームは、現在進行中の攻撃と新たな攻撃を積極的に察知し、侵害時間を最小限に抑え、緩和までの時間を短縮します。

お客様のチームを強化
Hunt のエキスパートが、貴社チームに代わって、貴社環境での攻撃の有無を監視し、時間と労力、コストの削減に貢献します。

迅速な対応
検知された重大なインシデントは直ちに通知されるため、安心して自社の本来業務に集中できます。

カスタマイズされた脅威ハンティング
Hunt チームは、貴社環境に対する攻撃を継続的に監視することで、基準となるセキュリティ設定を導き出し、特定のトポロジに合わせてハンティング手法をカスタマイズできます。

Akamai

豊富なコンテキストを駆使した脅威インテリジェンス

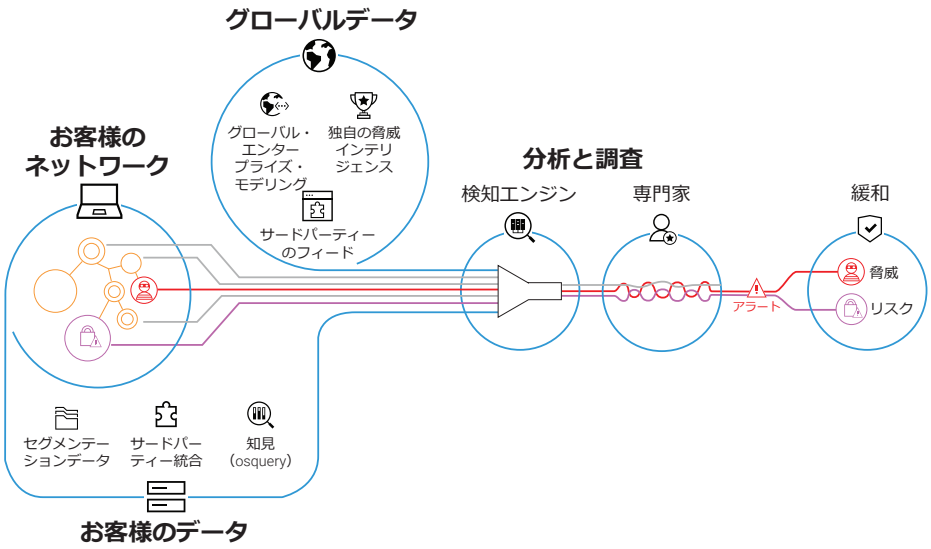
Akamai の Hunters チームが、Akamai Guardicore Segmentation と Akamai の大規模なグローバル脅威インテリジェンスを活用し、IP やドメインからプロセス、ユーザー、サービスに至るまで、さまざまな侵害の指標を収集しています。

ネットワーク、クラウド、エンドポイントの可視性

Akamai Guardicore Segmentation の導入で生成されたデータと Akamai のグローバルセンサー（Akamai DNS クラウドに対して発信される毎日 7 兆件以上の DNS リクエストを含む）を組み合わせることで、Akamai のチームはお客様の環境を非常に包括的に可視化します。

迅速な通知とプロアクティブな知見

- 脅威を検知すると、直ちに脅威に関するメール通知が送信されます。
- エグゼクティブレベルの定期脅威レポートは分析、統計、指標をまとめています。これによりエグゼクティブや経営陣は目立った攻撃キャンペーンを把握できます。
- Akamai Guardicore Segmentation コンソールとの統合により、インシデント管理が容易になりました。



> データ漏えいの検知と速やかな修復をサポートしてくれた Akamai Hunt チームには心から感謝しています。おかげで、当社のミッションクリティカルなシステムへのセキュリティ侵害を防ぐことができました。
>
> **CIO**
> 大手医療センター

Akamai Hunt およびその他のセキュリティソリューションの詳細については、エキスパートにお問い合わせください。

©2023 Akamai Technologies | サポート | 公開日：2023 年 3 月