MENLO SECURITY

HEAT Visibility
EXECUTIVE BRIEF

HEAT Visibility

組織を狙う高度に回避的な脅威を可視化し、実用性の高い脅威インテリジェンスを提供

ブラウザーが高度化するにつれて、攻撃者がブラウザーを標的とし、企業の検知機能を回避して行う攻撃も高度化しています。従来型のセキュリティソリューションは、ファイアウォールやセキュアWebゲートウェイが行うネットワークトラフィックの分析に依存していますが、これらには最新のWebセッションを含むさまざまなイベントを捕捉するために必要な可視性が備わっていません。攻撃者はこのことを知っており、HEAT（Highly Evasive Adaptive Threats：検知回避型脅威）と総称される、斬新かつ成功率の高いアプローチを用いて、これらのソリューションよりも優位に立っています。これらの回避的な脅威は、主要な攻撃ベクトルとしてWebブラウザーを標的にしており、従来型のネットワークベースソリューションおよびエンドポイントソリューションを回避します。これらのソリューションはブラウザー内で発生するイベントの可視性に欠けるため、検知回避型脅威は非常に深刻なものとなっています。

Menlo SecurityのHEAT Visibilityは、ブラウザーが直面している検知回避型脅威の実用的な脅威インテリジェンスに関する可視性と洞察を提供するため、組織はユーザーの安全性を高めるために必要な情報を得ることができます。HEAT Visibilityは以下を提供します：

- **従来型のソリューションでは検知できない検知回避型脅威を可視化：**他のセキュリティツールでは検知できない、高度に回避的な脅威を可視化します。またセキュリティチームはダッシュボードでの分析を行うことができ、リスクを理解しセキュリティ体制を向上させることができます。

- **回避的な脅威に関するインテリジェンスをSOCチームに統合し、インシデントレスポンスを迅速化：**さまざまな検知回避型脅威の手法についての実用的なアラートと充実した脅威インテリジェンスを提供し、インシデントレスポンスを改善します。検知回避型脅威に関するインテリジェンスはログAPIとSplunk TAを介してお客様のSIEM、SOAR、SOCプラットフォームに直接取り込まれ、セキュリティ対応のプレイブックの一部として使うことができます。

- **セキュリティポリシー制御の最適化：**セキュリティソリューションを回避するための戦術は進化し続け、新しい脅威が次々に発見されます。HEAT Visibilityは、お客様がポリシーの誤設定を特定し、回避的な攻撃のリスクを軽減するための追加の推奨事項を提供します。

製品概要

Menlo SecurityのHEAT Visibilityはお客様のWebログを自動で解析します。そして回避的な戦術の存在を示唆する悪意のあるWebおよびファイルへのリクエストを特定し、Menlo Securityの管理ポータル内の実用的なアラートおよびダッシュボード分析を通じて情報を提供します。これによりSOCチームは、精度の高いアラートという形で、実用的なフォレンジックレベルの情報を得ることができます。

特徴は以下の通りです：

HEAT攻撃ダッシュボード

MFAを回避するフィッシング攻撃やHTMLスマグリング、LURE（Legacy URL Reputation Evasion：レガシーURLレピュテーション回避）、悪意のあるパスワード保護ファイルなどの、他のソリューションでは検知/ブロックできない、ユーザーを標的とした高度に回避的な脅威を使うフィッシングやマルウェアについてのインテリジェンスを提供します。

Webログを継続的にスキャンし、実用的な洞察とアラートを提供

毎月4,000億件以上のアイソレーションされたWebセッションから、ドメイン、URL、IP、ブラウザーのテレメトリ、ユーザー行動、ファイルダウンロードなどのデータを分析し、ブラウザーを標的としたHEAT攻撃について包括的に可視化します。

実用性のあるHEATアラートとレポート

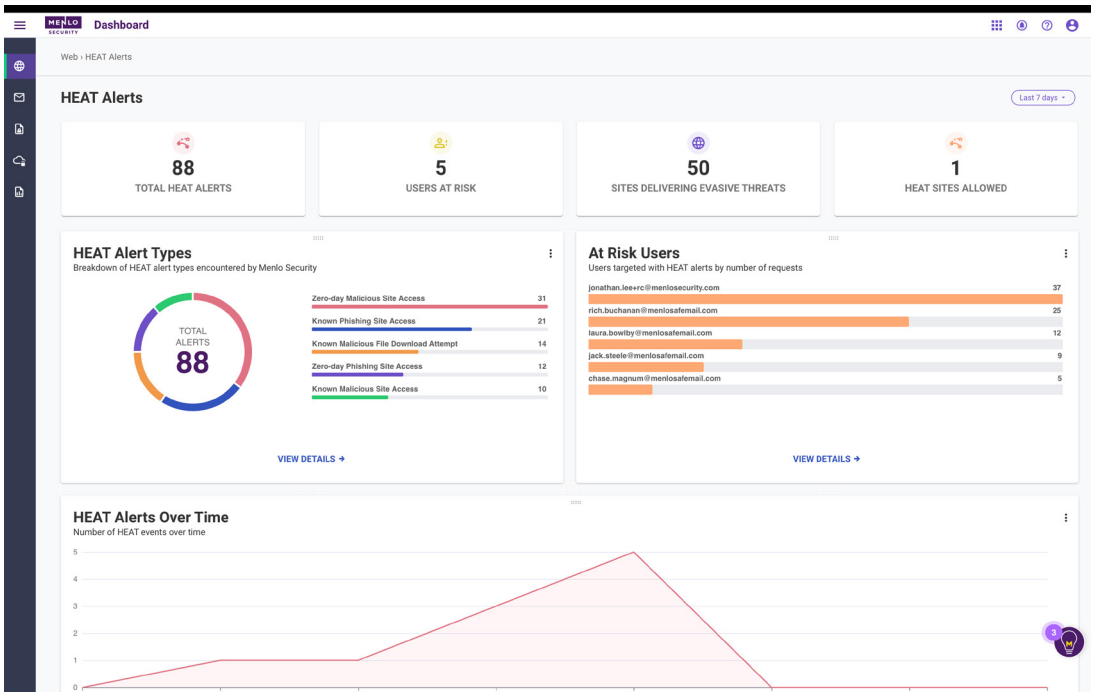
検知回避型脅威を検知した場合には、セキュリティチームにアラートが表示されます。脅威のタイプには、ゼロアワーのフィッシングサイトへのアクセスとパスワード送信、ゼロアワーの悪意のあるサイトへのアクセスおよびファイルへのアクセス、ゼロアワーのファイルダウンロード、既知のフィッシング/悪意のあるサイトへのアクセス、既知の悪意のあるファイルダウンロード、コマンド&コントロール（C2）トラフィックなどがあります。お客様はこれらのアラートを利用して、Menlo Securityプラットフォームから得られる脅威インテリジェンスを運用に活かすことができます。

ブロックリストにIOCを自動的に追加

ドメインやURLの情報は、自動的にMenlo Securityのグローバルブロックリストに追加されます。

ログエクスポートのためのAPIを用意

HEATのインテリジェンスをお客様のログ収集、自動化、セキュリティオーケストレーションツールに統合します。



お客様がWebページにアクセスすると、そのトラフィックはお客様のネットワークからMenlo Securityのクラウドプラットフォーム（インラインに配置され、疑わしい活動を見つけ出す）に送信されます。検知回避型脅威による攻撃を可視化することで、お客様は重大な脅威に対する初期調査から封じ込めまでを迅速に行うことができます。またセキュリティチームは、ログAPIや洞察に関するレポートおよび分析ツールを通じて検知回避型脅威のアラートを利用することができます。これによりお客様は脅威のトレンドを可視化し、Menlo Securityでブラウザーを保護することのビジネス価値を証明することができます。

Menlo Securityでブラウザーを保護

Menlo SecurityはHEAT Visibilityと共に、セキュアWebゲートウェイのすべての機能を、アイソレーションを活用したクラウドセキュリティプラットフォームに統合しており、Webやメール、そしてSaaSアプリケーション全体に堅固なセキュリティを提供します。これにはHEAT ShieldやRBI（Remote Browser Isolation）、CASB（Cloud Access Security Broker）、DLP（Data Loss Prevention）、プロキシ、Firewall-as-a-Service、プライベートアクセスなどが含まれ、拡張可能なAPIやポリシー管理、レポート作成、行動ベースの脅威分析のための単一のインターフェースを提供します。

お問い合わせ：
www.menlosecurity.com/ja-jp
japan@menlosecurity.com

Menlo Securityについて

Menlo Securityは、他に類を見ないアイソレーションを活用したクラウドセキュリティプラットフォームにより、企業が脅威を排除し、生産性を完全に維持することを可能にします。Menlo Securityは、悪意のある攻撃を防ぐために最も安全なゼロトラストアプローチを採用し、エンドユーザーはセキュリティの存在を気にせずにオンラインで仕事をすることができ、さらにセキュリティチームの運用負担を軽減することでクラウドセキュリティの目標を実現できる唯一のソリューションとなっています。これにより、企業は安全なオンライン体験を提供することができ、ユーザーは安心して業務を行いビジネスを進めることができます。

© 2023 Menlo Security, All Rights Reserved.