VECTRA
SECURITY THAT THINKS.®

データシート

Vectra Stream : 進化するネットワークメタデータ

Vectra Stream™ によって、セキュリティアナリストや脅威ハンターは、拡張性に優れたネイティブなクラウド、ハイブリッドクラウド環境、または企業内のトラフィックから取得したセキュリティ情報で強化した、拡張性に優れたメタデータを使って、明確な根拠に基づくインシデント調査を実施することができます。

現在のセキュリティデータは、バラバラに散在した状態にあります。NetFlowは不完全であり、PCAPはストレージやパフォーマンスを集約したものに過ぎません。オープンソースのZeekを採用した企業は、ハードウェアやソフトウェアの導入や設定、既存のツールとの連携といった、多くのリソースと時間を要する作業を強いられる状況になっています。言うまでもなく、セキュリティの専門家はこうした状況を肯定的にとらえていません。

Vectra Streamによってセキュリティチームは、カスタムツールや、脅威の検知、調査、ハンティングのためのフィードモデルの構築に必要となる豊富なネットワークコンテキストを活用することができます。また、オープンソースのZeekの利用においては避けられないオーバーヘッドや拡張性の制約に縛られることなく、セキュリティに関するインサイトを、Zeekフォーマットでデータレイクや SIEMにシームレスに提供することができます。

さらに、ホストIDを補完したメタデータによって、IPアドレスではなく、デバイス名を使って調査を行えることもVectra Streamのメリットです。これにより、特定の時間に該当するIPアドレスを使ったデバイス検索や、調査対象期間におけるIPアドレスの変更を、複数のDHCPログを見比べながら追跡する必要がなくなります。このデバイス名による検索は、スピードが重要となる局面において、大きな時間の節約につながります。メタデータに埋め込まれたセキュリティインサイトは、脅威ハンターに対して、調査や脅威ハンティングに必要な最新のインテリジェンスを提供します。

セキュリティ情報で強化したクラウドネットワークメタデータを、データレイクやSIEMに提供し、独自のカスタムモデルを作成することができます。

ハイライト

- 検索可能なメタデータを、Kafka、syslog、Elasticなど、好みのデータストアにZeekフォーマットで転送することができます。
- セキュリティに関する最新のインサイトで強化したメタデータによって容易な調査が可能となります。
- 脅威の検知、調査、ハンティングのためのカスタムツール、モデルを構築。
- 既存のZeekツールを全て活用することができます。
- クラウドとネットワークのメタデータをデータレイク内でホストとデバイスからのデータ（アプリケーションログ、プロセス、メモリなど）と関連付けます。
- 容易な導入：パフォーマンスのチューニングや継続的な保守は不要です。
- Zeekの単一センサーに比べて5倍以上のパフォーマンスを発揮します。

脅威ハンティングとインシデント調査の支援

- **実用的なネットワークデータをZeekフォーマットで提供。** Vectra Streamは、クラウドや企業内から数百のメタデータ属性を抽出し、既存のツールを使用してコンパクトでわかりやすいZeekフォーマットで表現します。Streamでは、NetFlowよりも詳細な情報を、フルパケットキャプチャのような複雑なストレージ機能不要でアナリストに提供することができます。
- **最新のセキュリティインサイトの活用。**機械学習によってセキュリティに関するインサイトを生成してメタデータ(ビーコン活動やドメインの希少性など)に取り込み、これを脅威ハンターが独自の専門知識と組み合せることで、強力なビルディングブロックを構築し、速やかに結果を獲得することが可能となります。
- **特権アクセス分析 (Privileged Access Analytics) の活用。**振る舞いを自動分析し、AIを利用して特権を持つエンティティを特定し、承認された使用と悪意を持つ使用を区別します。Privileged Access Analyticsは、Vectra®プラットフォーム全体で活用でき、Vectra StreamとVectra Recall™ では検索可能なセキュリティ強化機能として、Vectra Detect™ では検知機能として利用することができます。また、Vectra REST APIを通じてその属性にアクセスすることで、カスタムユースケースもサポートできます。
- **IPアドレスではなく、ホストをベースにした調査の実施。** Vectra Streamは、ネットワークメタデータを他の属性と自動的に関連付け、独自のホストIDを作成します。これによりセキュリティアナリストは、ホストのIPアドレスに変更があった場合でも、ホストを効率的に調査し、ホストグループ間の関係を容易に把握することが可能となります。
- **容易な設定と継続的なパフォーマンス。** Vectra Streamの設定はわずか30分未満で完了し、その後もパフォーマンスのチューニングや継続的なメンテナンスなしに、Zeekの単一センサーの5倍のパフォーマンスを発揮することができます。これにより、セキュリティチームはオープンソースのZeekを管理するためのオーバーヘッドを生じさせることなく、調査に集中することができます。

Vectraプラットフォーム

正確なコンテキストを備えた価値あるデータ

Vectraは、ネットワークの検知および対応における業界のリーダーです。クラウド、データセンターからユーザー、IoTデバイスに至るまで、これらすべてを横断した包括的なサイバー攻撃の検知は、もはやレガシーなテクノロジーでは対応不可能です。Vectraプラットフォームは、ネットワークのセキュリティに革命をもたらします。

高度なAIをベースに開発されたVectraプラットフォームは、ネットワークメタデータを収集・保存し、これらを適正なコンテキストで強化することで、既知の脅威だけでなく、未知の脅威さえリアルタイムに検知、追跡、調査することが可能になります。

Vectraプラットフォームは、分散アーキテクチャーで構成される最大規模のエンタープライズネットワークにも容易に対応できます。物理、仮想およびクラウドのセンサーを組み合わせ、クラウドやデータセンター、またユーザーやIoTのネットワークをあらゆる角度から横断的に可視化します。

Vectraプラットフォーム上で提供される3つのアプリケーションによって、優先度の高いユースケースに効果的に対応します。Vectra Streamは、最新のセキュリティ情報で強化したネットワークメタデータを、データレイクやSIEMに提供します。Vectra Recall は、セキュリティ情報で強化されたメタデータを使って脅威を調査するための、クラウドベースのアプリケーションです。AIをベースに開発されたVectra Detectは、隠れた未知の攻撃を迅速に検知して、優先順位付けを行います。

Vectra Streamの動作の仕組み

強化済みメタデータをデータレイクに転送

Vectra Streamでは、全てのパケットからメタデータを抽出し、検索や分析のためにデータレイクまたはSIEMに保存して、ネットワークトラフィックを可視化することができます。ネットワーク上でIPを使用する全てのデバイスを特定し、トラッキングします。

この可視化は、サーバーやラップトップ、プリンター、BYOD、IoTデバイス、またオペレーティングシステムやアプリケーション、さらにはデータセンターとクラウドの仮想ワークロード間のトラフィックにまで及びます。メタデータには、脅威のハンティングやインシデント調査において重要な意味を持つ、コネクティビティやプロトコル全体の詳細が含まれます。

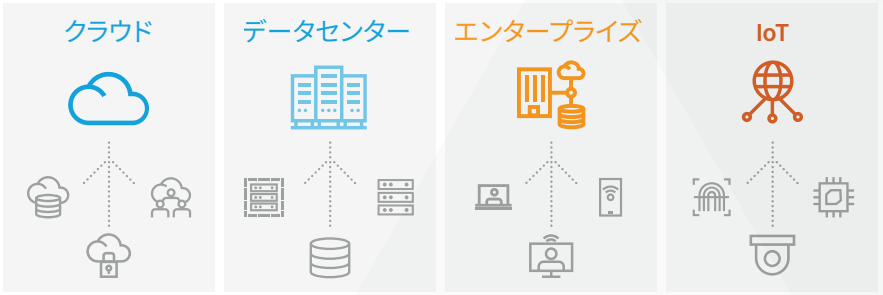
メタデータは、すべての内部のトラフィック（横方向）、インターネットとのトラフィック（縦方向）、仮想インフラストラクチャーのトラフィック、クラウドコンピューティング環境のトラフィックから取得されます。Vectra Streamは、検索可能なメタデータをKafka、syslog、Elasticなど、好みのデータレイクに転送します。

Vectraプラットフォームを使った容易な導入

Vectraプラットフォームは、30分以下の時間で導入が可能で、センサーインフラストラクチャー管理のためのオーバーヘッドを発生させることなく、脅威のハンティングやインシデントの調査を開始できます。

物理または仮想センサーが、キャンパスやデータセンター、クラウドなど、ネットワークの異なる構成要素からメタデータを収集します。

センサーはセンターに存在するエンティティ（Brain）に接続し、Brainはフローの重複排除を行って、ホストの特定とデータ強化のためのアルゴリズムを実行します。Vectra Streamは、オンプレミスの仮想マシン（VM）として展開されます。VMはメタデータをZeekフォーマットに正規化して、オンプレミスやクラウドにあるデータレイクやSEIMに提供します。



Vectraは、攻撃者に隠れる場所を与えません

脅威のハンティング

侵害の痕跡 (IoC: Indicators of Compromise) は、アナリストの日々のワークフローや、組織内での共有、あるいは内部調査を目的に使用されるオープンソースインテリジェンスにおいて発見されます。アナリストは、IoC強化済みのネットワークメタデータを検索することで、サイバー攻撃の過程で使用されるIPアドレスやドメイン、URL、ハッシュ、SSL証明書を遡及的に調査することができます。長期間保存されているメタデータを使ったIoC検索は、大きな意味を持ち、同時に非常に強力な武器となります。

ネットワークとホストデータの関連付け

効果的な脅威のハンティングは、ITアセットやリスク、企業ネットワーク内のフローの包括的な可視化によって実現します。このような可視化に必要となるデータは、以下の3つのカテゴリーに分類できます。

- ネットワークメタデータによってホスト間の全ての通信を可視化することで、ユーザーやデバイス、ワークロード、IPアドレス、ドメインといった、エンティティ間のネットワークを横断する全てのやり取りを明らかにすることができます。脅威ハンターは、これらのやり取りを基にネットワーク内の攻撃者の活動を特定することができます。
- ホストデータによって、ユーザーアカウントのアクティビティやシステム処理など、システム環境内のホストで発生したイベントを可視化することができます。
- アプリケーションデータセットは、システム環境内で稼動するプログラムのイベントログです。

ネットワークメタデータは、アナリストにネットワーク全体で発生したパターンやイベントに対するハイレベルなビューを提供します。

ホストとアプリケーションデータ（つまり、デバイスデータ）は、アナリストにシステムプロセスやメモリアクセスなど、ホスト単位のきめ細かなローレベルの詳細情報を提供します。

これらのデータセットを組み合わせることで、想定される様々な事象の総括的なマップを提供することができます。また、これらのデータセットによって脅威ハンターは、高度な脅威についても効率的に検出できるようになります。

脅威の検知、調査、ハンティングのためのカスタムツール、モデルの構築

アナリストはカスタマイズされた独自の検知機能によって、疑わしい脅威や新たな脅威、コンプライアンス違反、内部の誤用や業界固有の攻撃など、あらゆる種類の活動に対するイベントを監視することができます。Vectra Streamのセキュリティに関するインサイトは、メタデータに取り込まれた機械学習のビルディングブロックを提供します。これを他の属性と組み合わせることで、特定のホストやユーザーアカウントに関連付けた、強力なカスタムモデルを作成することができます。

確証性に優れたインシデント調査

Vectra Streamによって、セキュリティアナリストはデータレイクやSIEMに存在するデータに関する、さらに詳細で精度の高いインシデント調査を驚異的なスピードで進められるようになります。

セキュリティアナリストは、強化済みのネットワークメタデータによって、Vectra Detectやサードパーティのセキュリティ製品が検知した一連の攻撃内容や、過去のネットワークメタデータにある高品質な脅威インテリジェンスを容易に利用することができます。

Vectra Detectアプリケーションやサードパーティのセキュリティ製品からインシデントが報告されると、Vectra Streamはセキュリティアナリストに対して、全てのワークロードとデバイスのアクティビティを全方位で確認できるビューを提供します。

これにより、セキュリティアナリストは、ネットワーク全体のトランザクションに関する完全なコンテキストや、関連するデバイス、アカウント、ネットワーク通信に関する詳細な情報に基づいて、かつてないほどのスピードでインシデントを調査できるようになります。

お問い合わせ：info-japan@vectra.ai　vectra.ai/jp