VECTRA
SECURITY THAT THINKS®

データシート

Vectra Detect：サイバー攻撃をリアルタイムに検知・阻止するための最も強力なソリューション

Vectra®が提供する、サイバー攻撃の検知と脅威追跡のためのプラットフォームのコア機能を担うVectra Detect™は、クラウドやデータセンター、さらに企業のIT環境に対するサイバー攻撃を、極めて迅速かつ効率的に検知して阻止するためのソリューションです。Vectra Detectでは、AIを活用することで外部からの攻撃をリアルタイムに可視化し、攻撃の詳細な情報を提供します。

進行中の攻撃に対する迅速かつ明確な対応を支援するだけでなく、Vectra Recall™を利用することで、詳細な調査を行う脅威追跡の専門家に対しても、重要な開始箇所（スターティングポイント）を提示することができます。

ディープラーニングやニューラルネットワークなど、高度な機械学習技術と常時学習型の振る舞いモデルを組み合わせたVectra Detectによって、実際に被害が発生する前に、隠れた未知の攻撃者を迅速かつ効率的に発見することが可能になります。

Vectra Detectは、クラウドからエンタープライズ、認証システム、SaaSアプリケーションに至るまで、全てのネットワークトラフィックを分析して、企業全体に潜在するサイバー攻撃を可視化します。これにより、クラウドやデータセンターのワークロードからIoTデバイスに至るまで、攻撃者は身を隠す場所がなくなります。

お客様は、Vectra Detectのサブスクリプションによって、新たな脅威の検知アルゴリズムに関するアップデートを定期的に受け取ることで、最新の高度な脅威にも継続的に対応することができます。

Vectra Detectによって、実際に被害が発生する前に、隠れた未知の攻撃者を迅速かつ効率的に発見することが可能になります。

39 **サイバー攻撃は39秒に1回発生**

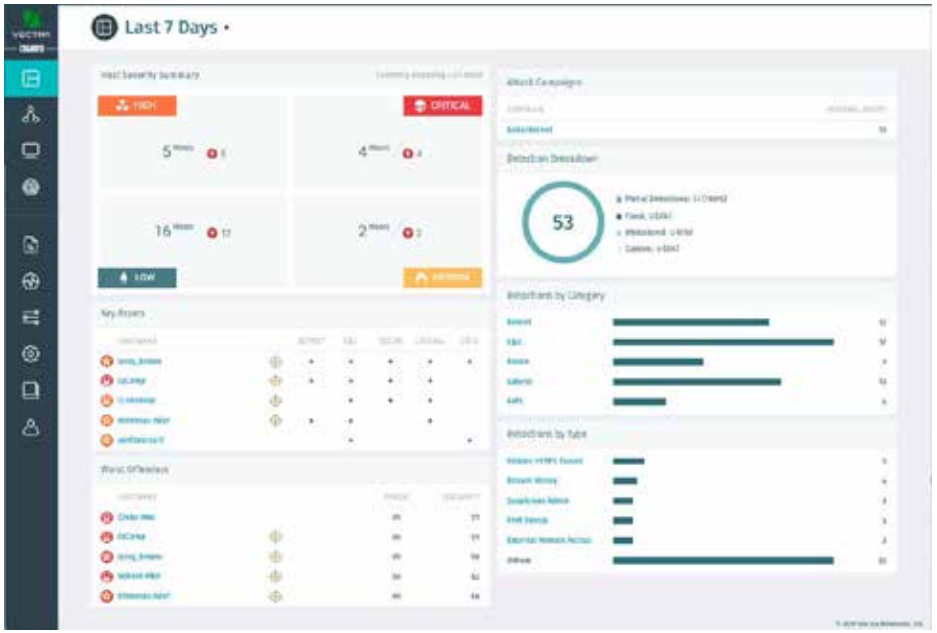
防御だけでは、必要とされるセキュリティ対策にはなりません

ハイライト

- AIを活用した常時学習型の振る舞いモデルによって、隠れた未知の攻撃を検知し、迅速かつ確実な対応を可能にすると共に、AIのアシストによる脅威の追跡によって、最初に確認すべき箇所を明確に示すことができます。
- AIの活用と主要な脅威インテリジェンスソースとの連携によって、既知の脅威を速やかに検知します。
- セキュリティ強化ネットワークメタデータや関連するログ、さらにクラウドのイベントを分析することで、全てのクラウド環境、データセンターのワークロード、ユーザー、そしてIoTデバイスに対する攻撃者の振る舞いを可視化します。
- 独自のコンテキストによって、脅威に対する終わりの見えない追跡を不要なものとし、また事前に密接な関連性を持つ情報を提供することで、脅威に対する即時の対応を可能にします。
- EDRやNACファイアウォール、その他の実施ポイントを利用することで、新種の脅威についても確実にブロックします。
- Vectra Recall、SIEM、さらにフォレンジックツールを使ったより広範な調査に対しても、明確な開始箇所を提示することができます。

ソフトウェアのセキュリティアナリスト

Vectra Detectはサイバー攻撃を自動的にハンティングして、その隠れ場所と活動内容をレポートします。リスクの高い脅威については瞬時にトリアージされ、ホストとの関連付けを行って優先順位付けされるため、セキュリティチームは、進行中の攻撃にも迅速に対応でき、データの喪失を回避することができます。



攻撃者の存在が検知された場合、瞬時に優先順位付けとスコアリング、そして侵害されたホストデバイスとの関連付けが行われます。

Vectra Detectは、クラウドや企業のトラフィックをリアルタイムに可視化します。

Vectra人口知能

Vectra Detectは、数週間から数ヶ月を要する手作業によるセキュリティイベントの分析を、自動化によってわずか数分に短縮し、セキュリティアナリストによる脅威の調査効率を37倍まで高めることができます。

これにより、人員不足に悩まされ、またサイバー攻撃に遅れを取らないためのプレッシャーに晒されてきたセキュリティオペレーションチームは、隠れた脅威に対して迅速に対応できるようになります。

豊富なメタデータ

- ネットワークトラフィック
- システム、認証、SaaSログ
- IoCs（STIX）

攻撃者の振る舞いを特定

- 機械学習
- 振る舞い分析
- ネットワーク効果

自動分析

- トリアージと脅威のホストへの関連付け
- リスクに応じたホストの優先順位付け
- アタックキャンペーンの発見

対応の加速

- 豊富なコンテキストを備えた直観的なUI
- 対応の自動化
- ファイアウォール、エンドポイント、SIEMおよびNACの連携

Vectra Detectの動作の仕組み

豊富なメタデータ

Vectra Detectは、パケットの詳細な調査を行うことなく、パケットからネットワークメタデータを抽出することによって、クラウドや企業のトラフィックをリアルタイムに可視化し、迅速な保護を可能にします。

メタデータ分析は、横方向も含めた全ての内部のトラフィック、インターネットとの縦方向のトラフィック、また仮想インフラストラクチャー、クラウド環境に対しても実施されます。これにより、クラウドからエンタープライズに至るまで、IPを使用する全てのデバイスを特定し、トラッキングとスコアリングを実施します。

このような可視化は、ラップトップやサーバー、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、SaaSアプリケーション間のトラフィックにまで及びます。

システムや認証情報、そしてSaaSのログを使って、ネットワークメタデータのコンテキストを補強し分析することで、システムやユーザーをより正確に特定することができます。

Vectra Detectでは、STIXの脅威インテリジェンスが提供する、既知の侵害の指標を利用して、脅威を検知します。さらに、その結果を他の攻撃者の振る舞いと関連付けることで、脅威をピンポイントで正確に特定し、確実なスコアリングでリスクの優先順位付けを行うことができます。

Vectra Detectは、継続的にローカル環境を学習し、全てのクラウドおよびオンプレミスホストをトラッキングすることで、デバイスの侵害やインサイダーによる脅威の兆候を明らかにします。

攻撃者の振る舞いを特定

Vectra Detectは、隠れた攻撃者、あるいは未知の攻撃者を特定するための振る舞い検知アルゴリズムを使って、収集したメタデータを分析します。これにより、リモートアクセスツールや隠れたトンネル、バックドア、認証情報の不正使用、内部情報の流出、横方向への移動など、クラウドやエンタープライズトラフィックにおける攻撃者の基本的な行動が明らかになります。

Vectra Detectは、クラウドからユーザーやIoTデバイスに至るまで、あらゆる範囲の脅威を検知します。

Vectra Detectは、継続的にローカル環境を学習し、全てのクラウドおよびオンプレミスホストをトラッキングすることで、デバイスの侵害やインサイダーによる脅威の兆候を明らかにします。攻撃ライフサイクルの全てのフェーズで、以下のような様々なサイバー攻撃を自動的に検知します：

- コマンドアンドコントロールや隠れた通信
- 内部の偵察
- 横方向の移動
- アカウント認証情報の不正使用
- データの流出
- ランサムウェア攻撃の早期段階での兆候
- ボットネットによる収益化
- 全てのホストのマッピングや関連する攻撃指標などの攻撃キャンペーン

Vectra Detectは、権限を持つ従業員による重要なアセットに対する不審なアクセスの監視と検知、さらにクラウドストレージやUSBストレージの使用や、その他の手段を使ったネットワーク外へのデータの移動といったポリシー違反の監視と検知も行います。

セキュリティ洞察機能により、セキュリティアナリストは、環境内の新しいアカウント、ホスト、その他のデバイス（IoT）を追跡・評価し、新しいデバイスやアカウントによるネットワークアクセスや新しい管理プロトコルの使用などの非セキュリティ情報を表面化させることができます。

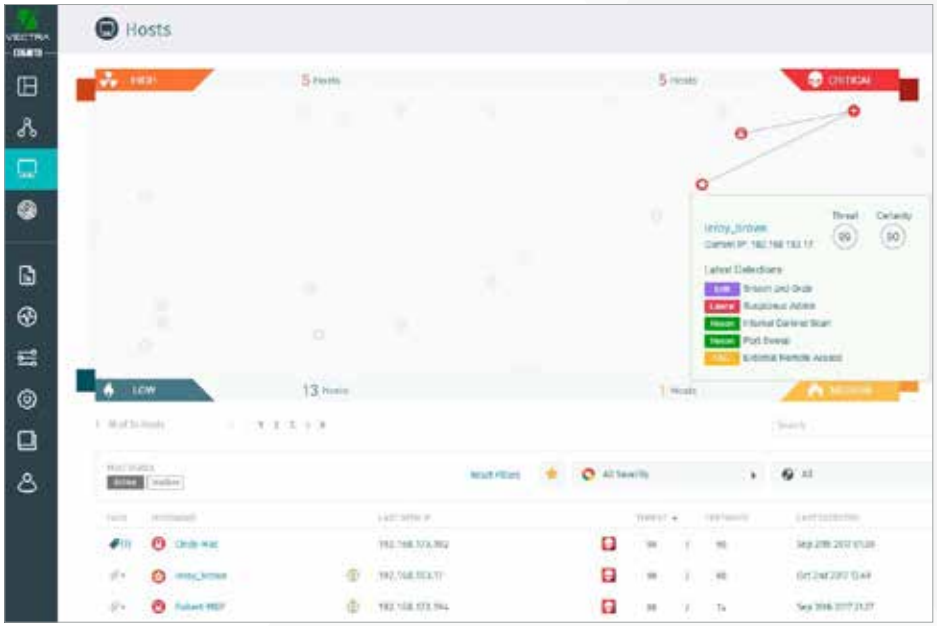
Vectraは、新しいアカウントを自動的に識別し、実行する役割（ドメインコントローラやDNSサーバなど）によりホストにラベルを付けます。これにより、検知に伴うリスクをより適切に評価し、十分な情報を得た上で対応することができます。

自動分析

Vectra DetectのThreat Certainty Index™ は、数千におよぶイベントと過去のコンテキストを集約し、最大の脅威となるホストを特定します。

Vectra Detectでは、分析対象となるイベントを無制限に増やすのではなく、データを重要度に応じて絞り込みます。脅威の確信度を示すスコアを基にスタッフに対して通知を行うほか、他のエンフォースメントポイントやSIEM、そしてフォレンジックツールからの応答を促します。

Attack Campaign機能によって、散在する攻撃者の振る舞いの関連付けを行い、脅威が検出された内部のホストや高度なコマンドアンドコントロールが検出された外部のホスト、さらにコマンドアンドコントロールのためのインフラストラクチャーに共通するコネクティビティを明らかにして、さらなる検知の自動化を図ることができます。

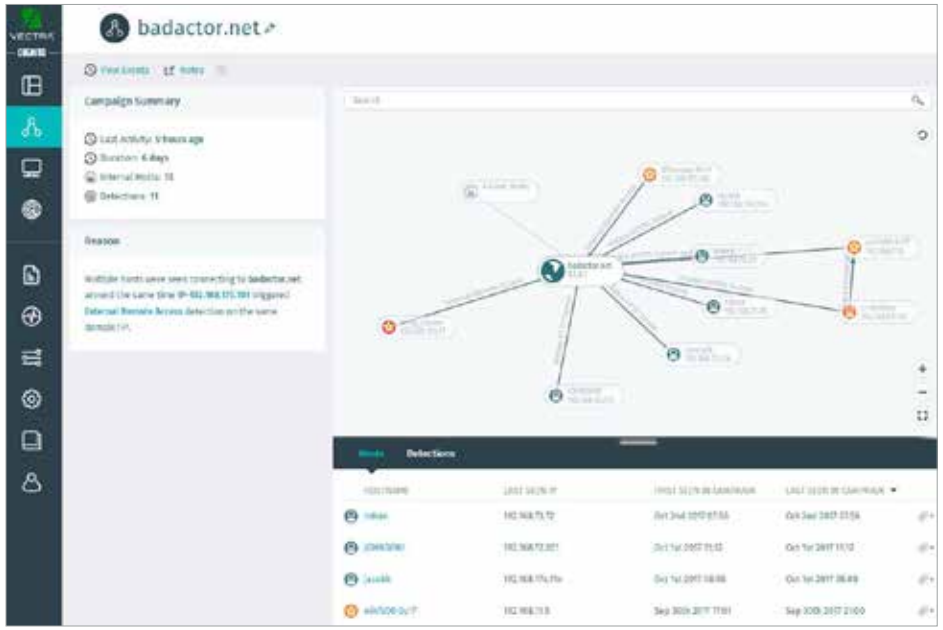


Vectra Detectが示す脅威の確度に関する指標 (Threat Certainty Index)。

攻撃者が偵察を実施して、ホストやクラウドのワークロードを横方向に移動しても、Vectra Detectは、振る舞いと検知結果の関連付けを行うことで、攻撃キャンペーン全体を総括して表示することができます。

また、ビューをホストや検知したキャンペーンに切り替え、過去の全てのイベントを分析することで、アクティビティや攻撃の全体像に対する理解を深めることができます。

Vectraは、コンテキスト全体の情報を1つの場所に集約して表示するため、他のツールに切り替える必要はありません。



Vectra Detectは攻撃キャンペーン全体を総括したビューの形で提供します。

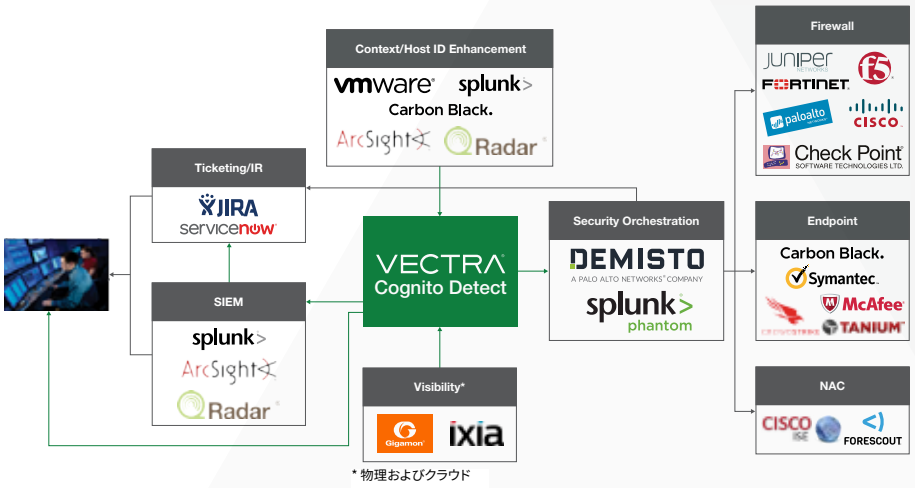
ホストのコンテキストやキャプチャしたパケット、脅威と確信度のスコアリングなど、検知した脅威の詳細をいち早く提供することも可能です。

対応の加速

Vectra Detectは、最も関連性の高い情報とコンテキストを提供することで、脅威に迅速かつ的確に対応できるようにします。市販のセキュリティ分析ツールとは異なり、手作業による調査ではなく、脅威の優先順位付け、侵害を受けたホストや攻撃の標的となっている重要なアセットとの関連付けを自動的に行います。

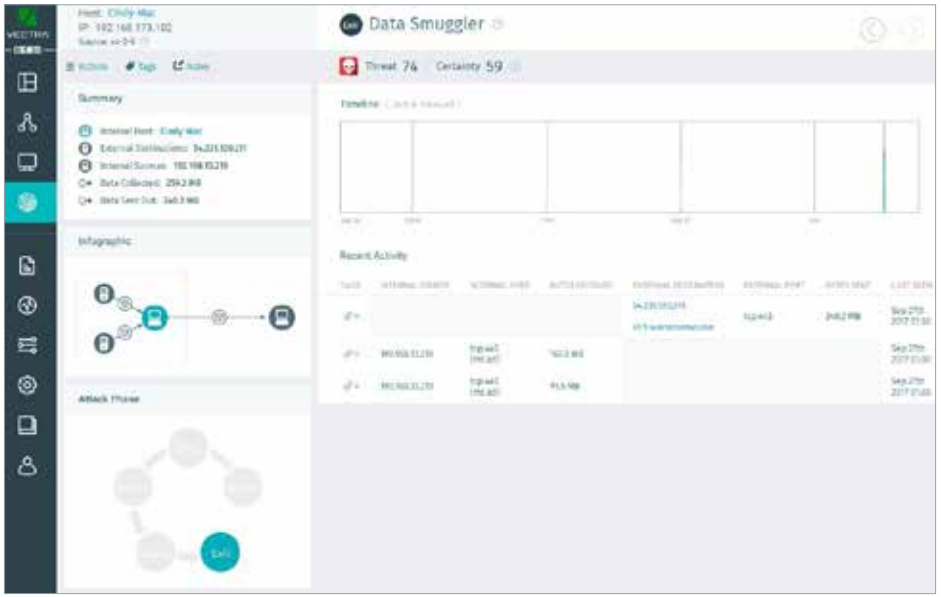
ホストのコンテキストやキャプチャしたパケット、脅威と確信度のスコアリングなど、検知した脅威の詳細をいち早く提供することも可能です。

また、Vectra Detectでは、既存の次世代ファイアウォールやエンドポイントセキュリティ、NAC、その他のエンフォースメントポイントと連携し、未知のカスタマイズされたサイバー攻撃も自動的に阻止することができます。さらに、脅威ハンティングの開始箇所を明確に提示することで、SIEMやフォレンジック分析ツールの効率をさらに高めることができます。



Vectra Detectでは、幅広く利用されているエンフォースメントポイントやSIEM、フォレンジック分析ツールとの連携が可能です。

自ら思考するセキュリティソリューション (Security that thinks®)



進行中のデータ流出をリアルタイムに検知。

セキュアなコンテキストによる時間の節約

Vectra Detectは、人員が不足しているセキュリティオペレーションチームの負荷を大幅に軽減します。長い時間を要するセキュリティイベントの分析が自動化され、終わることのない隠れた脅威のハンティングが排除されることによって、これが可能になります。

またVectra Detectでは、検出した結果の詳細に加えて、その根拠となるイベントやコンテキストの履歴などを提示します。セキュリティアナリストは、任意のホストのコネクションマップを瞬時に表示して、デバイスが他のどのようなホストとの間で、どのように通信しているのかを確認することができます。

Vectra Detect は、ネットワークおよびクラウド上のアカウントの統一ビューを提供できる唯一のソリューションです。このプラットフォームは、ワークロードとID間の相互作用を認識および評価し、環境内でどのように機能しているかを把握することができます。

さらに、Vectra Detectは、フォレンジック分析のためにキャプチャしたパケットからリッチメタデータにオンデマンドでアクセスすることも可能です。これにより、即座に決断を下し、行動するために必要な証拠と正確性を得ることができます。

Vectra Detectは、振る舞いを自動的に分析する特権アクセス分析（Privileged Access Analytics）を活用。人工知能を用いて特権を持つエンティティを識別し、承認されている使用と悪意のある使用を区別します。これはVectraプラットフォーム全体で、Vectra StreamとVectra Recallでは検索可能なセキュリティエンリッチメントとして、Vectra Detectでは検知として利用できます。また、Vectra REST APIを通じて属性にアクセスすることで、カスタムユースケースをサポートします。

既存のセキュリティインフラストラクチャーの強化

ファイアウォールやエンドポイントセキュリティ、NACその他のエンフォースメントポイントを使って、新たなレベルの脅威をブロックするためのインテリジェンスを提供する場合、あるいはSIEMやフォレンジックツールを使って広範な調査を開始する場合でも、Vectra Detectは、既存のセキュリティテクノロジーからこれまでにない価値を引き出すことができます。

Vectra Detectは、最先端のエンドポイントセキュリティソリューションと連携することで、強化されたコンテキストを自動的に調査結果へ追加します。セキュリティオペレーションチームは、これを活用して侵害を受けたホストデバイスを隔離することができます。

また、強力なAPIを使って応答を自動化することで、実質的に全てのセキュリティソリューションとの連携も可能です。さらに、Vectra Detectは、全ての検知結果に対するsyslogメッセージやCEFログのほか、優先順位付けされたホストスコアを生成します。これにより、Vectra Detectのログは単純な他のログソース以上の効果を発揮し、SIEMによる調査やワークフローのための理想的な糸口となります。

ランサムウェアの全ライフサイクルを検知

Vectra Detectは、企業などに対するランサムウェア攻撃の全てのフェーズを特定する

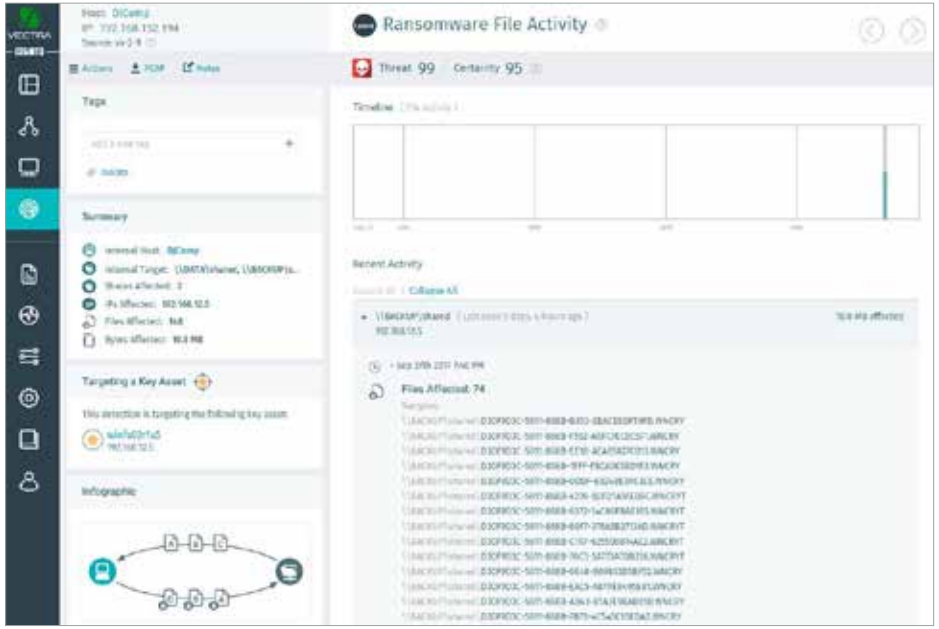
ことができます。内部のネットワークトラフィックを監視することで、重要な資産を人質に取ろうとするランサムウェア攻撃の基本的な振る舞いを、数秒以内に特定できます。

さらにVectra Detectは、ランサムウェアの直接的な検知に加えて、コマンドアンドコントロールトラフィックや、ランサムウェアが重要なアセットを見つけ出し、暗号化を試みる際のネットワークスキャンや拡散の振る舞いといった兆候も捉えることができます。

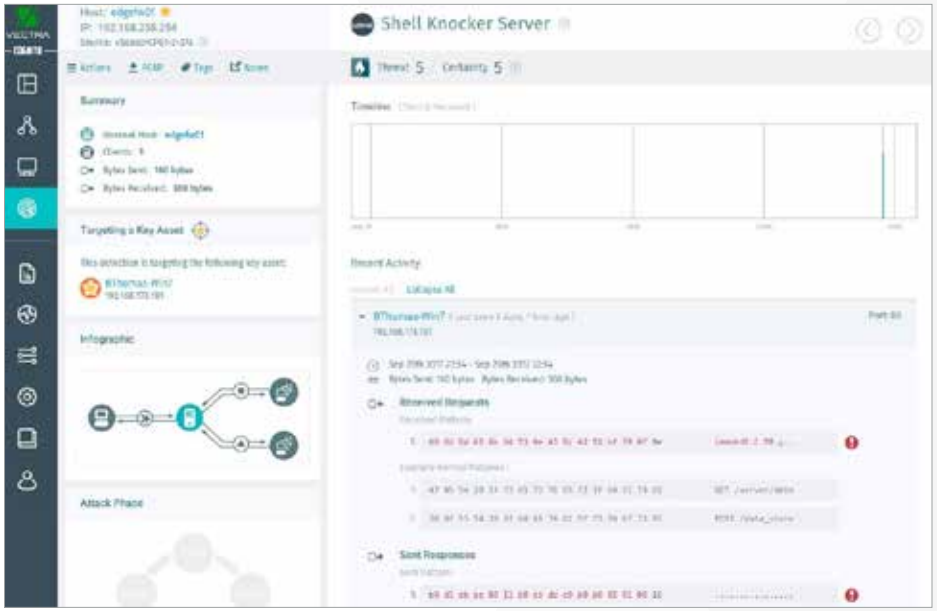
ウォッチャーを監視する

攻撃者が最初にエンドユーザーのデバイスを侵害できたとしても、システム管理者やシステムの認証情報を手に入れることができなければ、最終的な成果は得ることができません。Vectra Detectは、ユーザーの振る舞いを監視するだけでなく、システム管理者に対する侵害の兆候も捉えることができます。

Vectra Detectは、管理用のプロトコルをトラッキングして、特定のホストやサー



Vectra Detectによるランサムウェアの検知。



Vectra DetectによるShell-Knockerの検知。

バー、ワークロードの管理に使用されるマシンや踏み台となるシステムを学習します。これにより、攻撃者がシステム管理者の認証情報やプロトコルを使って企てるサイバー攻撃を、即座に明らかにすることができます。

データセンターの運用を統合

現代のデータセンターでは、ネットワークやアプリケーション開発、仮想化、そしてセキュリティ担当チーム間の調整を絶えず行っていく必要があります。全てのグループ間の同期を図ることができるVectra Detectによって、ワークロードが絶えず変化する状況でも、クラウドからエンタープライズまで完全な可視性を維持することができます。

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