VECTRA SECURITY THAT THINKS. | cybereason

ソリューション概要

Vectra＋Cybereason 完全な可視性、より迅速な対応

Vectra CognitoプラットフォームとCybereason Defense Platformの連携によって、より高度なサイバー攻撃の検知、防止、対応を実現します。Vectra AI社のクラウドネイティブなネットワーク検知機能とCybereasonの包括的なエンドポイント保護機能を組み合わせることで、エンドポイントからネットワーク全体のエンドツーエンドの可視性のために、データを簡単に相互に関連付けることができます。2つのソリューションを組み合わせることで、セキュリティの調査時間を短縮し、インシデントへの迅速な対応を可能にします。

ネットワークとエンドポイントの完全な可視性とコンテキスト

Vectra CognitoとCybereasonはAPIを介して連携し、ネットワークとエンドポイントのデータを共有します。これにより、セキュリティ担当者はCognitoプラットフォームから直接、拡張属性の可視性を得ることができます。そして、クラウド、エンタープライズ環境、エンドユーザーマシン、IoTデバイスにまたがる攻撃を簡単に関連付けることができるのです。

また、この共同ソリューションでは、Cybereason Malicious Operation - Malop™から対応する情報とコンテキストが提供されるため、攻撃の完全なタイムラインを取得し、影響を受けたすべてのユーザーとマシンの確認、および根本原因を特定し、悪意のある通信を発見することができます。また、ユーザーはVectra Cognitoから、影響を受けたホストに簡単に移行し、追加調査を行うことを可能とします。

チャレンジ

セキュリティ部門は、アラートの嵐に追われてしまうことがしばしばあります。アラートの優先順位が付けられていない場合は、トリアージにさらに時間がかかります。人員が十分に配置されているチームであっても、インシデントに関するネットワークデータとエンドポイントデータの間で可視性、相関性、およびコンテキストが不足していれば、調査に時間がかかり対応が遅れてしまいます。

ソリューション

Vectra CognitoとCybereason Defense Platformおよびその包括的なエンドポイント保護機能は、ネットワークとエンドポイントのデータを組み合わせて完全な可視性を取得し、迅速にサイバー攻撃への対応を行うことを支援します。

メリット

VectraとCybereasonの連携によって、エンドツーエンドのネットワークとエンドポイントの可視性を実現し、時間とセキュリティリソースを節約できます。優先順位付けされたアラート、自動相関データ、脅威のコンテキスト情報により、セキュリティ部門はインシデントを迅速かつ効率的に調査し、修正することができます。

ネットワークとエンドポイントの完全な可視性に加え、先を見越した脅威ハンティング機能により、攻撃者はどこにも隠れることができません。

調査・対応の迅速化

Vectra AIとCybereasonを連携させることで、追加の属性とコンテキストをすぐに使えるようにし、セキュリティ運用の作業負荷を大幅に軽減、より迅速な対応を可能にします。

データサイエンス、最新の機械学習技術、人工知能に基づく振る舞い分析を組み合わせたVectra Cognitoは、自動化された脅威ハンティングをノンストップで実行します。インシデントはパッケージ化されたフォレンジックで自動的に優先順位付けされることで調査が容易になります。実際、Vectra Cognitoによって、脅威の調査に費やす時間を最大90%削減できることが実証されています。対応者は、脅威の種類、リスクレベル、確実性に基づいて適切なアクションを起こすことができます。

Cybereasonとの連携により、エンドポイントの予防、検出、修復が可能になります。それによって、プロセスの停止、ファイルの隔離、ファイル実行の防止、マシンの隔離などを行い、サイバー攻撃を効果的に阻止し、エンタープライズ内でのラテラルムーブを防ぐことができます。

Vectra Cognitoによって、脅威の調査に費やす時間を最大90%削減できることが実証されています。

エンタープライズ対応と拡張性

Vectra AIとCybereasonの連携によるソリューションは、ハイブリッド、マルチクラウド、オンプレミスをサポートし、すべてのエンタープライズ環境に可視性を提供します。Vectra AIのクラウドネイティブプラットフォームとCybereasonの軽量エージェントの組み合わせは、現代のサイバー攻撃に対抗するために必要な最新のソリューションです。

またこの連携によるソリューションは、エンタープライズを導入初日から保護します。Vectra AIの高度な機械学習技術と振る舞いを常に学習するというモデルにより、初日から正確な検知と忠実度の高い結果を得ることができます。他のネットワーク検知ツールとは異なり、Vectra Cognitoは学習期間を必要としません。これをCybereasonのビルトイン脅威検知機能と組み合わせることで、セキュリティ部門は複雑な設定を行ったり、複雑かつ静的なルールを調整するのに時間を費やす必要がなくなります。

ネットワークとエンドポイントにまたがって広範囲の脅威から保護するため、Vectra AIとCybereasonの連携ソリューションを活用することで、脅威に対する完全な可視性を取得し、サイバー攻撃に迅速に対応することができます。

Vectra AIとCybereasonの連携によるソリューションは、ハイブリッド、マルチクラウド、オンプレミスをサポートし、すべてのエンタープライズ環境に可視性を提供します。

詳細については、Vectra AI社（info-japan@vectra.ai）までお問い合わせください。

Vectraについて

ネットワークの検知および対応（NDR）のリーダーとして、Vectra® AI は、データ、システム、インフラを守ります。Vectra AIは、SOCチームが攻撃者を迅速に発見し、攻撃が実行される前に対応することを可能にします。

Vectra AIは、オンプレミス、クラウドの両方において、拡張されたネットワーク上の不審な振る舞いやアクティビティを迅速に検出します。Vectra AIは、不審な動きを発見し、フラグを立て、セキュリティ担当者にアラートを発し、即座に対応できるようにします。

Vectra AIは、「自ら思考するセキュリティソリューション（Security that thinks®）」です。人工知能を使用して検知と対応を時間の経過とともに向上し続け、誤検知を排除することで真の脅威に集中することを可能とします。

Cybereasonについて

最先端のCyber Defense Platformの開発者であるCybereasonは、サイバーセキュリティへの全く新しいアプローチにより、防御側にアドバンテージをもたらします。Cybereasonは、エンドポイントの防御、検知、対応、そしてアクティブな監視を提供します。このソリューションは、既知および未知の脅威を防ぐためのシグネチャやシグネチャレスの技術と、ランサムウェアやファイルレス攻撃を防ぐための振る舞いや偽装技術を組み合わせて、多層的なエンドポイント防御を実現します。サイバー攻撃の第一線で培った技術を持つエリート・インテリジェンスの専門家によって設立されたCybereasonは、非公開企業としてボストンに本社を置き、ロンドン、シドニー、テルアビブ、東京、アジア太平洋地域、ヨーロッパ大陸にオフィスを構えています。

Email info-japan@vectra.ai