VECTRA
SECURITY THAT THINKS.®

データシート

Vectraの脅威検知および対応プラットフォーム

Vectraのネットワークの検知および対応プラットフォームは、AI駆動型で、攻撃を発見・阻止するための最も早く効率的な方法を提供します。

ハイブリッドアプリケーションやクラウドネイティブアプリケーション、AWSおよびAzure環境、Azure ADのIDを使用したMicrosoft Office 365などのSaaSアプリケーション、データセンターのワークロード、IoT、エンタープライズネットワークまでをカバーします。

Vectraプラットフォームは、組織にリスクをもたらす脅威の振る舞いに優先順位をつけ、実用的なデータと自動化された対応を提供します。それによって、どこからハンティングや調査を始めるべきか、常に明確に把握できます。

- クラウド、データセンター、IoT、エンタープライズネットワークの内部に潜むサイバー脅威を、自動的に検知し、優先順位をつけて対応します。
- クラウドとエンタープライズのインフラにまたがって大規模にメタデータを取得することで、脅威の検知を迅速化し、調査時間を短縮します。
- セキュリティメタデータを収集し、深い洞察力とコンテキストで強化することで、アナリストは幅広い攻撃シナリオを、早期に、かつ一貫して阻止することができます。
- Tier-1およびTier-2分析の手動タスクの自動化を利用して、セキュリティオペレーション全体の作業負荷を軽減することができます。
- セキュリティアナリストが積極的に脅威を発見し、インシデントを調査する時間が増えれば、進行中の攻撃を阻止することにつながります。
- セキュリティ洞察の統合・共有によって、レスポンスタイムを短縮化します。EDR、SIEM、SOARツールと連携し、エンドポイントからクラウドまでの脅威管理と可視化を実現します。

Vectraは、攻撃者に隠れる場所を与えません

AI駆動型のVectraプラットフォームは、パブリッククラウドやハイブリッドクラウドだけでなく、データセンターやIoTデバイスを含むエンタープライズネットワーク全体の攻撃も確認し、阻止するための最も早く効率的な方法を提供します。

脅威検知の自動化

機械学習から派生した常時学習型の振る舞いモデルを用いて、リアルタイムに脅威を検知します。特許取得済みのVectraのAIは、検知結果を特定のホストやアカウントと相関させることで、攻撃をより早く発見し、迅速に修復することを可能とします。

脅威ハンティングの強化

Vectraプラットフォームや、サードパーティのセキュリティソリューションで検知されたインシデントを、より深く、より広く調査するなど、積極的な脅威ハンティングをさらに効率的に実行します。

視認性の向上

セキュリティが強化されたネットワークメタデータ、関連するログ、クラウドイベントを収集・分析・保存することで、すべてのワークロード、サービス、サーバー、ホストデバイス、アカウント、ロール、ユーザーの行動を、これまでにないほど可視化できます。

一度のキャプチャーで何役もこなす

単一のプラットフォームからセキュリティを強化したメタデータにアクセスすることで、脅威の検知やインシデント対応を自動化するとともに、調査やAIを活用した脅威探索を加速させることができます。

Vectraプラットフォームは、すべての検知結果、ホストやアカウントのスコア、メタデータにAPIを介してアクセスすることができ、パートナーやベンダーに依存しないことを目指しています。これにより、セキュリティ担当者は、最高のソリューションを活用して、真のエンタープライズスケールかつ世界で通用するセキュリティインフラを構築することができます。

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