verizon

Network Detection& Response

クラウドから提供されるフルパケットキャプチャのソリューションにより、ほぼリアルタイムで、または過去に遡り、脅威を検知して可視化します。

どのようなインシデントが、どこで、どのくらいの規模影響しているか、またそれを即座に把握できていますか？

1
IT環境、ネットワークの一部しか可視化できておらず、ログ収集も不十分

2
ログ監視によるアラート通知は受けているが、解析する必要があり、時間がかかる

3
IoT, OTなどログがでない端末の分析ができていない

Verizon NDRがそのような状況を解決します

従来のソリューション、ログ、エージェントを利用した対策だけでは自社環境の一部しか可視化できませんでした。内部の端末が踏み台にされる攻撃手法も増える中、カバー範囲を圧倒的に広げます。

- ✓ パケットベースでのネットワーク監視
- ✓ リアルタイムでの相関分析と結果の可視化
- ✓ サイバーキルチェーンに基づいた脅威の各ステージを分類して表示

- ✓ インシデントやその予兆、影響範囲を視覚的に把握
- ✓ すぐにトリアージや対応策実施などアクションに移すことができる
- ✓ 事前・事後の「通常の通信」も可視化するため、より深い調査にも対応

Verizon NDRの特徴

・ネットワークからエンドポイントまでの脅威を分析、可視化し脅威への即時対応を可能に
・リアルタイムだけでなく、過去を遡った分析も自動で実行
・クラウドサービスだから、高価なオンプレ機器の導入は不要。

各機能の紹介

Network Memory	・フルパケットキャプチャおよびリプレイ、長期間の保持と解析 ・複数のパケットキャプチャパターン（フルパケット、ストリームヘッドのみ、ネットフローのみ） ・プロトコルやIPアドレスレンジでのキャプチャ指定も可能 ・センサー(パケットキャプチャ用ソフトウェア)数の上限なし ・既存セキュリティツール群との API 連携も可能
Wisdom Engine	・4,000 種類以上のプロトコル/アプリケーションに対するディープパケットインスペクション ・IT系プロトコルのみならずOT系プロトコルにも対応 ・自社保有の脅威情報に加え、サードパーティが提供する脅威情報も解析に使用 ・サイバーキルチェーンの各ステージにあわせた脅威評価 ・IDS、レピュテーション、File Hash、Cert Hash、JA3、ヒューリスティックスなどを駆使した先進的な検知と相関分析 ・メタデータ、ネットフロー、ペイロードなどあらゆる観点でトラフィックを分析
Visualizer	・従来のCUI的、あるいは静的ダッシュボードによるUIに対して一線を画した美しく、動的、かつ日常運用をスマートに行える可視化インターフェイス ・月単位から分単位までこまかくスケールを変えることのできるタイムライン設定・過去への遡りもカーソルをドラッグ＆ドロップするだけ ・インシデントに関連したIPアドレスやデータストリームを直感的にわかりやすく表示

利用料金について	Verizon NDRは年間ライセンスで提供されます。検査対象とするデータ量によってライセンス料金が異なります。詳細はお問い合わせください。

株式会社パロンゴ
▸ HP：https://parongo.com
▸ Email：sales@parongo.com

インフラストラクチャとしての
セキュリティオペレーションの実現へ

PARONGO
— internet security company —