Verizon NDRのご紹介(NDR: Network Detection and Response)

PARONGO
– internet security company –

◆ 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応を可能に
- ✓ リアルタイムのみならず遡っての分析もフルオートで
- ✓ 高価なオンプレ機器は不要。クラウドサービスとしてご提供

～ Verizon NDR　3つのポイント　～

セキュリティ運用効率化

“Event”化されたアラート通知を提供。時系列、IPアドレス等、検索カテゴリにより、複数の角度からのインシデント分析・解析を可能とし、セキュリティ対応へ迅速につなげることが可能。

豊富な脅威インテリジェンス及びレガシー技術との連携

脅威インテリジェンスと既存技術と融合された情報を元に、より信頼できる情報が提供される。AIだけでは判断しづらい通常／異常通信を認識し、トリアージに活かせる。企業独自にルール作成し、不要アラート排除も可能。

内部および新領域リスク対応

外部からだけでなく、内部から外部、内部間での攻撃についても検知・分析が可能。NAT配下やBYOD等の端末への通信可視化・特定も可能となるため、ゲスト端末含めたリスクマネジメントへつなげることが可能。IoT(OT)等、ログがでない端末も対象となる。

どんなインシデントが、“どこで”、“どれくらいの規模・影響なのか”“どのような対応が必要なのか”即座に把握できていますか？

従来のソリューションではIT環境の一部のみしか可視化できていない。ネットワークを網羅的に可視化ができていないためログ収集が不十分。

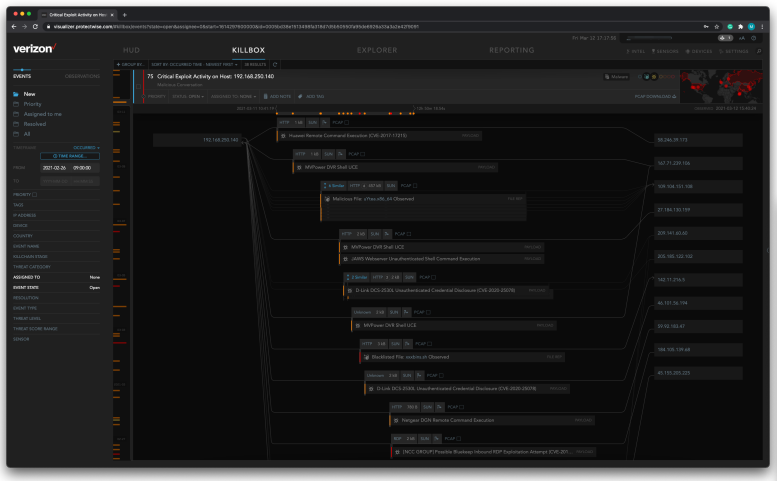
ログ監視によるアラート通知からは、ログ・その他情報を突き合わせて解析する必要があるため時間がかかる

IoT(OT)等、ログがでない端末はどう分析する？

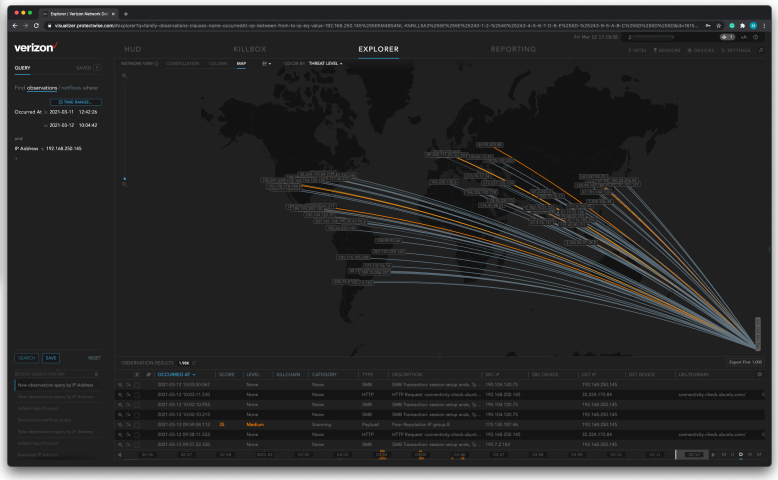
Verizon NDRがそのような状況を解決します！

- ログベースではなく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

株式会社パロンゴ：https://www.parongo.com
email：info@parongo.com



KILLBOX:
インシデントの概要、Dst IP/Src IP、トラフィックの中身などを一覧し、何が起こっているのかを瞬時に把握



EXPLORER:
IP アドレスや HTTP Query Strings など細かな条件に合致する通信状況を可視化し、インシデントの広がりや当該エンドポイントがどこと通信しているのかといった詳細についても可視化

項目	機能説明
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	• 4000 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 • 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 • IP アドレスやプロトコル、インシデント名など多数の条件でタイムラインを検索 • インシデントに関連する IP アドレスをクリックだけで派生しながら可視化

◆ Verizon NDRで実現！

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行動に移すことができる → 事前事後の「通常の通信」も可視化し、より深い調査に対応

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IT環境の一部しか可視化できません。
内部端末が踏み台にされ、インシデントにつながるケースも拡大しています。