Recorded Future®

マルウェア対策ツールの性能比較
Recorded Future vs. VirusTotal Enterprise

既存のマルウェアスキャナーと比較した、統合型マルウェアインテリジェンスの強みとは？

	Recorded Future®	VirusTotal
ドロップされたファイルを実行する動的サンドボックス	◉ 1日150万件以上のファイルの動作分析およびC2追跡による脅威の完全な可視化	○ 複数のサンドボックスによる解析が可能だがファイルデトネーションは含まれない
自然言語検索（NLS）	◉ あらゆる質問に対して文脈を理解した回答を提供	○ キーワードベースのクエリのみに対応
NLS、TTP、IOC、行動パターン別にサーチ可能な高度検索	◉ マルウェア、脅威アクター、IOCに関する最新情報を提供	○ YARAルールまたはIOCの検索のみが可能
YARAルールの自動生成	◉ 新出のマルウェアファミリーを特定するためのYARAルール自動生成が無制限に利用可能で、手動作成が不要に	○ 基本的なパターンの提案はあるが、手動作成が必要
リスクスコアリング	◉ マルウェアの特性に基づく、周辺情報を含んだ動的なRecorded Future Risk Scoreを提供	◉ AVエンジンによる検知数の静的カウントのみを表示
脅威の属性と全体的な脅威状況の把握	◉ マルウェアの脅威アクター、MITRE TTP、攻撃対象インフラを特定し、攻撃チェーン全体の可視化を実現	○ Google CTIの情報を転用
優先順位付けされたアラート	◉ マルウェアの挙動や特性、アクターのTTPを基にアラートを発出	◉ アラート通知は脅威がアセットのウォッチリスト（VT Alerts）やYARAルールに該当した場合（Livehunt）のみ
他社サービスとの統合	◉ 柔軟なAPIを搭載し、Google SecOps（Google Chronicle）、Splunk Enterprise、Sentinel、Palo Altoなどと統合可能	◉ 統合可能なサービスが限られ、統合先を追加するには手動でのスクリプト作成が必要

◉ 高度な機能　◉ 一般的な機能　○ 提供なし

Recorded Futureは世界最大の脅威インテリジェンス企業です。Recorded FutureのIntelligence Cloudは、攻撃者からインフラストラクチャ、攻撃対象までをカバーするエンドツーエンドのインテリジェンスを提供します。当社はインターネット全体にわたってオープンウェブ、ダークウェブ、およびテクニカルソースから情報を収集し、拡大を続けるアタックサーフェスと脅威ランドスケープをリアルタイムで可視化することで、お客様が迅速かつ迷わずに問題に対応し、リスクを軽減し、安全にビジネスを成長させていくためのお手伝いをします。ボストンに本社を置き、世界中に拠点を擁するRecorded Futureは、80カ国以上の1,900社を超える企業や政府機関の委託を受け、実用的で偏りのない、最新のインテリジェンスを提供しています。詳細はrecordedfuture.comをご覧下さい。