ThreatSonar ANTI-RANSOMWARE

エンドポイントの検出応答

企業、政府機関、組織のサイバーセキュリティチームは、サイバー攻撃を検出、調査、軽減する際に多数の課題に直面しています。サイバーセキュリティチームは、様々なエンドポイントから収集される膨大なデータに見合った分析および調査能力が必要です。さらに、ハッカー攻撃は大量の情報に埋もれてしまうことが多く、セキュリティ担当者が本当の疑わしい攻撃を特定するのに時間がかかってしまいます。そのため、インシデント対応と調査が遅れ、生産性に影響を及ぼし、運用コストが増加してしまいます。

インテリジェンス主導のエンドポイントセキュリティで組織のサイバー攻撃に対する防御力を強化

グルーバルな脅威インテリジェンスの長期的な研究と悪意のあるプログラムの追跡をしてきた TeamT5 は、企業、政府、組織のサイバーセキュリティ防御の必要性を深く理解しており、脅威インテリジェンスによる攻撃の継続的な予測、異常な動作の常時監視を行う ThreatSonar Anti-Ransomware エンドポイント検出応答プラットフォームを開発しました。脅威を検出すると、即座に警告を出して攻撃行為を遮断し、効果的にインシデントに対応するので、侵入による被害を軽減できます。

利点

- **効果的なサイバーセキュリティ保護**
  高い検出範囲で、潜在的な脅威を正確にブロックします。
- **対応時間の短縮**
  自動で脅威を分析し、インシデント対応を迅速化します。
- **アラート疲れの緩和**
  サイバーセキュリティ担当者のリスクレベル評価を支援し、リスクの高いインシデントの処理に集中できるようにします。
- **担当者の検出負担の軽減**
  自動化されたインテリジェントな脅威ハンティングにより、環境に潜む脅威を積極的に発見します。
- **インシデントの緩和、損失の最小化**
  ラテラルムーブメントを防止し、脅威による損害を修復します。

特徴

① 常時監視により脅威を見過ごさない

エンジンの自己学習メカニズムにより、よく使用されるプログラムや新しい悪意のあるプログラムを自動的に識別し、暗号化されたファイルを効果的に検出します。

② イベントの軌跡を即座に特定するための可視化

攻撃経路を可視化することで、イベントの軌跡を調べ、イベント情報でタグ付けできるので、サイバーセキュリティアナリストは迅速に攻撃者の行動を特定および深く理解し、緩和処置をすることが可能です。

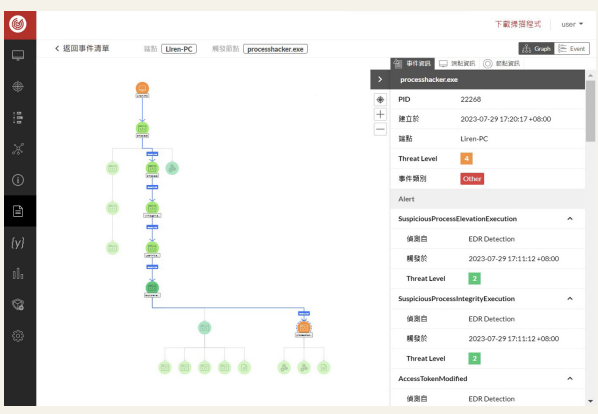
③ MITRE ATT&CK® を活用した攻撃調査の迅速化

各セキュリティイベントは関連する ATT&CK の戦術とテクニックにタグ付けされているため、サイバーセキュリティチームは特定の攻撃グループに対する防御の効果を即座に評価できます。

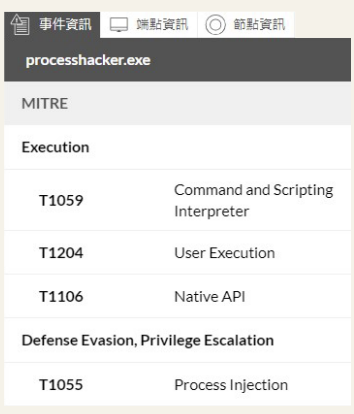
④ タイムラインによるインシデント全貌の表示とインシデント調査時間の短縮

ノードとイベントの二種類のタイムラインを通し、前後のインシデント記録を分析し、インシデント調査を迅速に行うことができます。

② サイバーキルチェーンの可視化

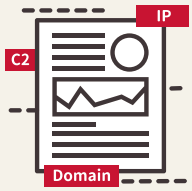


③ MITRE ATT&CK® の活用



④ タイムラインによるインシデント調査

ThreatSonar はどのようにランサムウェア攻撃を包括的に防ぐのか？

脅威の予測 ▶ セキュリティ侵害前	▶ セキュリティ侵害時	▶ セキュリティ侵害後
			
インテリジェンス 脅威インテリジェンス	**エンドポイント** 新しいプログラムの監視	**ブロック** リアルタイム応答	**復元** バックアップファイルの保護

今後の攻撃を継続的に予測し、的確に防御

TeamT5　脅威インテリジェンスチームが主要なハッカーグループの最新の攻撃手法を長期的に追跡することで、最先端のインテリジェンスを活用し、ランサムウェア攻撃の次のステップを予測します。

ランサムウェアを積極的に追跡し、即座に攻撃をブロック

何百ものランサムウェアプログラムを識別し、保護されたファイルの周辺にトラップファイルを仕掛けることで、不正なプログラムがアクセスしようとした場合、自動的に対策措置を発動し、即座にソフトウェアを終了させ、悪意のあるプログラムによるファイルの暗号化を阻止します。

脅威の拡散を食い止め、即座に隔離措置を実施

リスクの高い脅威が検出されると、即座にアラートが発せられます。脅威インテリジェンス分析によって攻撃と判断された場合は、悪意のあるプログラムを停止してエンドポイントを隔離し、攻撃者によるネットワーク内での横方向の移動を防ぎます。

悪意のある破壊を阻止し、バックアップデータを効果的に保護ならびに復元

Windows VSS サービスにより、バックアップメカニズムを迅速に有効にします。ThreatSonar はバックアップを破壊しようとする悪意のある動作を積極的に検出すると、即座にブロックし、企業や組織がデータを正常に復元できるようにします。

TeamT5 について

政府機関、テクノロジー、製造、金融、医療、軍事、電気通信、その他の業界を含む、世界中の 300 を超える顧客から広く信頼されています。

TeamT5 は、マルウェアと高度な持続的標的型攻撃 (APT) とマルウェアに関する 20 年以上の経験があります。言語と文化的な利点により、当社はアジア太平洋地域におけるサイバースパイ活動に関する具体的な専門知識を有しており、米国の Black Hat や日本の Code Blue / AVTokyo 、ドイツの Troopers 、そして Hack In The Box と FIRST を含む、世界クラスのサイバーセキュリティカンファレンスで最新の研究を発表するため頻繁に招待されています。また、脅威インテリジェンスの研究と先進的なサイバーセキュリティ技術の分野で世界をリードするチームとして、当社は米国の Bloomberg と CNN 、日本の産経新聞と朝日新聞、韓国の ET News からインタビューを受けています。

TeamT5株式会社 営業部 ▌ E-mail sales-admin-jp@teamt5.jp ▌ Tel 080-3550-8829