Datasheet

ThreatSonar

TEAMT5

ThreatSonar 脅威フォレンジック分析プラットフォーム

インテリジェンス主導の脅威フォレンジックによる APT 攻撃の検出
APT (持続的標的型攻撃)の攻撃方法は日々変化し続けています。多くの場合、攻撃が発見された時には企業の重要機密情報は既にハッカーの手中にあります。したがって、脅威攻撃の早期検出とラテラルムーブメントの時間を短縮することは、脅威フォレンジックの主な課題となります。

ハッキング対策も感染症対策のようにインテリジェンスを活用し、隠れた APT 脅威を積極的に追跡

ハッキング対策は感染症対策に似ています。企業、政府、組織は脅威や攻撃を防ぐため、ファイアウォールによる外部からの遮断、アンチウィルスソフトの導入による受動的な自己防御など、感染症対策時に行う水際対策や流行の蔓延を防ぐためのマスク着用などのように、さまざまな対策を行っています。しかし、企業、政府、組織の情報環境が安全かどうかは、クイックフォレンジックによる確認が必要です。

防御措置	外部遮断	自己防衛	安全性の確認
感染対策	水際対策	マスク着用 / ソーシャルディスタンス	検査キット
サイバーセキュリティ脅威に対する防御	Firewall, IPS, WAF	エンドポイント保護	ThreatSonar

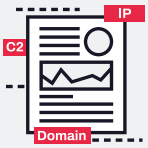
TeamT5 チームは長年にわたり世界的な脅威インテリジェンスを研究し、悪意のあるプログラムを追跡しており、企業、政府、組織のサイバーセキュリティ脅威防御のニーズを熟知しています。また、脅威行動分析、先進的なテクノロジーや実際の事例によって訓練された独自の APT リスクモデルを使用し、ThreatSonar 脅威フォレンジック分析プラットフォームを開発しており、サイバーセキュリティを迅速にチェックならびに検証し、隠れた侵入脅威を正確に発見します。

	検出	採用	実装
重要な利点	1,000件以上	90%以上	100万以上
	他社製品では検出できなかった APT 攻撃	台湾のマネージドセキュリティサービスプロバイダー(MSSP)	エンドポイントフォレンジック

- **柔軟性のあるデプロイメント**
  オンプレミスとクラウド管理メカニズムを備えており、複数の仮想基盤と互換性があります。
- **ハッカーグループが頻繁に使用する隠れたTTP脅威の積極的な検出**
  世界的な脅威インテリジェンスの研究によって裏付けられ、悪意のあるプロセスを正確に特定し、侵入攻撃を早期検出ならびに未知の攻撃を予防します。
- **迅速で効率的なフォレンジック**
  十分なハードウェアリソースがある場合、大規模なフォレンジック(5000 以上のエンドポイント)を 1 時間で実行できます。
- **検出と対応時間の短縮**
  自動調査により類似した攻撃手口(TTPs)による隠れた感染を分析し、インシデント対応の実行を迅速にします。
- **OSのサポート**
  Windows, Linux, MacOS

ThreatSonar 脅威フォレンジック分析

データ収集と調査



高度な脅威ハンティング技術により、エンドポイント上の疑わしいプログラムとファイルアクティビティを発見し、潜在的脅威を特定します。

インテリジェンス主導フォレンジック

IOC と脅威インテリジェンスの相互関係を通し、特定されたイベントを検証します。

根本原因分析

インシデントがどのように発生したか判断し、脅威を特定します。

フォレンジックレポート

特定された脅威と根本原因を含みます。評価中に行われたすべての活動と決定は、今後の参考のために記録されます。

業界をリードする機能

インテリジェンス主導のスマートな脅威フォレンジック

何千もの APT バックドアインジケータを内蔵しており、脅威フォレンジックのために最新のインテリジェンスを各エンドポイントに提供します。また、ハッシュ、IP、ドメイン、Yaraルール、IoC などの外部インテリジェンスをインポートし、潜在的な標的型攻撃の脅威から守ります。

日々の運用に影響を与えない軽量なデプロイとバックグラウンド実行

ThreatSonar 実行可能プログラムは企業内の何千台ものコンピュータに導入できる且つ少ないシステム リソースで実行できます。よって、担当者はフォレンジックを実行する負担を負うことなく、通常どおりコンピュータ作業を行うことが可能です。

侵害評価によるインシデントの全体像の把握、調査時間の短縮

ThreatSonar はホストのストの状態を分析するだけではなく、ログ分析を通して過去のイベントの軌跡を調査およびタイムライン上に一連のイベントを表示し、そしてクロスエンドポイントの相関を通してラテラルムーブメントとデータ流出経路を追跡します。

未知の悪意のあるプログラムを効果的に特定するためのメモリフォレンジックと行動分析を完備

メモリ内に隠された悪意のあるプログラム、実行済みおよび実行予定のプログラム、攻撃者のハックツール、ホスト上の攻撃後のログを特定し、数百もの活動的な動作異常を自動的に特定します。

侵害された可能性のあるエンドポイントの相関の可視化によるアクティブな脅威ハンティング

統計的相関分析により未知の攻撃方法を発見および異常な動作を追跡するためのベースラインを確立し、組織内の稀なプログラムや合法的なシステムツールの悪用、またはデジタル署名付きマルウェアなどの潜在的な未知の脅威をマークします。

TeamT5 について

v.202605

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 550 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。

E-mail sales-admin-jp@teamt5.jp

TEAMT5 | THREAT INTELLIGENCE PIONEER, BORN IN ASIA