ThreatSonar

能動的に潜伏脅威を見つける
脅威ハンティングツール

▶ アンチウイルスだけではマルウェアの侵入を防ぐことは難しい

既知のマルウェアに対してはほぼ100%の検知率を誇るアンチウイルスソフトも、未知や亜種のマルウェアの検知は苦手としています。

▶ 24時間365日常時監視を行う「EDR」でも、潜伏脅威の発見は難しい

EDRはエンドポイントに侵入した高度なマルウェアを検知し、被害を最小化するためのソリューションです。その検知手法は“異常な挙動”に対してアラートを発呼する仕組みとなります。その特性上、潜伏脅威を見つけることは苦手としています。

ThreatSonarとは？

EDRと同じくエンドポイントに侵入した高度なマルウェアおよび潜伏脅威を検知するための製品です。
EDRとの違いは、侵害された可能性のある「状態」の有無をチェックし脅威を検知する点です。

不審なプログラムの生成 | **レアなプログラムの自動起動設定** | **無効化されたセキュリティ設定**

※上記のような「状態」を発見した場合に、Threat Levelを判定し５段階でレポートします。

▶▶▶ 3つの製品比較 ◀◀◀

	AV	EDR	ThreatSonar
防御フェーズ	侵入前	侵入後	侵入後
ターゲット	既知のマルウェア	未知のマルウェア APTマルウェア	未知のマルウェア APTマルウェア
検知手法	パターンマッチング	Behavior Analysis （「行動・挙動」をチェック）	Forensic State Analysis （侵害されたと思われる「状態」の有無をチェック）
製品の特長	・インストール要。PoC要 ・他のセキュリティ製品と競合	・インストール要。PoC要。 ・他のセキュリティ製品と競合	・インストール不要のため導入が容易 ・他のセキュリティ製品と一緒に利用可能
長所と弱点	・未知のマルウェアに弱い ・ファイルレス攻撃に弱い	・24時間365日の常時監視が基本 ・潜んでいるマルウェアの特定は苦手 ・正規挙動の切り分けのため他のイベントとの相関分析が必要。EDRに相関分析機能がない場合にはSIEMが必要となる ・攻撃者はEDR導入不可の端末やシャドウITを攻撃の起点する傾向あり。 ・攻撃者は挙動を隠したり、プロセスの親子関係を任意に設定することが可能で、EDRの検知を免れる手法あり	・常時監視ではなく、スキャン時にマルウェアを検知 ・スキャン時間が短く、PCに与える負荷も小さい ・潜んでいるマルウェアを見つけることが得意 ・数千台から数万台を同時に調査することが得意 ・APTマルウェアの情報を検知ルール化(YARAルール)しているため、ATマルウェアの検知率が高い ・他のセキュリティ製品と競合しないため、EDRと一緒に利用し、機能を補完しあうことが可能

TEAMT5 TeamT5株式会社　営業部 | sales-admin-jp@teamt5.jp | 080-3550-8829

ThreatSonar

能動的に潜伏脅威を見つける
脅威ハンティングツール

▶▶▶ 製品の特徴 ◀◀◀

- 提供ライセンスは1年契約のseatライセンスとスポットスキャン用のcreditライセンスあり
- Forensic State Analysisにより、AVやEDRが見逃してしまった脅威を見つけることが可能
- EDR導入済のお客様でも、EDR＋ThreatSonarの同時利用が可能
- 管理コンソールはオンプレ運用とMSSP提供のクラウド運用の2種類あり
- スキャンエージェントはオフライン環境でも利用可能なオフラインモードもあり

製品導入の流れ

01

- 製品提案の実施
- お見積りの提示

02

- デモライセンスによるPoCの実施(レポート結果の確認)

03

- 申し込み申請書の提出
- 申請後、2営業日以内にライセンスを発行

TeamT5とは

※ 蔡英文さん、オードリータンさんの前でスピーチをする
弊社代表のツァイ・ソンティン(TT)

- 2014年に台湾法人を設立。今年で10期目
- 台湾の5名(T5)で始まった会社が現在150名＋
- 創業からずっと、極東アジアのサイバー攻撃組織の監視、情報収集、分析を行い、その結果をレポートとして提供
- 2022年6月に日本法人設立。
- 2022年9月にJAFCO　ASIA、伊藤忠商事、マクニカ社よりシリーズAの資金調達を完了

TEAMT5 TeamT5株式会社　営業部 | sales-admin-jp@teamt5.jp | 080-3550-8829