Datasheet

ThreatSonar ANTI-RANSOMWARE

TEAMT5

サイバー脅威による攻撃を可視化し、エンドポイントに包括的な多層防御を実現

ThreatSonar Anti-Ransomware EDR プラットフォーム

企業や政府機関、各種組織のセキュリティチームは、サイバー脅威の予防・検知・対応において以下のような様々な課題に直面しています。

- 多層防御（Defense-in-Depth）をエンドポイントまで拡張し多層的な脅威検知と保護の実装
- 限られた検知能力の中での、高度な攻撃やゼロデイ攻撃への対応
- 疑わしい脅威やインシデントの迅速な調査、被害の早期抑制

利点

- **高精度な脅威検知**
  被害が発生する前に潜在的な脅威を正確に検知し、ブロックします。
- **コンテキストを踏まえた調査**
  攻撃の動きを自動的に分析し、調査および対応を迅速化します。
- **アラート疲労を軽減**
  不要なアラートを排除し、セキュリティチームがよりリスクレベルの高い脅威に集中できるようにします。
- **脅威の封じ込めを自動化**
  不正な活動を停止し、環境全体への被害拡大を防ぎます。
- **侵害の影響を最小化**
  ラテラルムーブメントを阻止し、攻撃の影響を最小限に抑えることで業務上の損失を減らします。

ランサムウェア対策のためのインテリジェンス駆動型のエンドポイント防御

TeamT5 は長年にわたる脅威リサーチとセキュリティ分野での専門知識を活かし、インテリジェンス駆動型の Endpoint Detection and Response（EDR）プラットフォーム、ThreatSonar Anti-Ransomware を提供しています。
実践的な脅威インテリジェンスを基盤として、本プラットフォームはエンドポイントのリアルタイム可視化、脅威検知、自動対応機能を提供し、APT 攻撃・マルウェア・ランサムウェアなどの悪意ある活動を特定・阻止します。疑わしい挙動が検知された場合、システムは即座にアラートを発し、調査を行うとともに、攻撃活動をブロックすることでセキュリティインシデントの影響を最小限に抑えます。
また、ThreatSonar Anti-Ransomware は、組織が NIST CSF （Cybersecurity Framework） に準拠したセキュリティ対策を実装できるよう支援し、エンドポイントにおける多層防御（Defense-in-Depth）の強化に貢献します。

識別	防御	検知	対応	復旧
脅威インテリジェンスを活用し、エンドポイントのリスクを可視化	自動化された防御により、既知・未知の脅威からの攻撃を事前に阻止	不審な行為を継続的に監視し、リアルタイムで検知	集中管理によりインシデント対応を迅速化	システムの運用復旧を行い、インシデント分析の知見を活用して防御体制を強化

主な特徴

包括的なエンドポイント防御

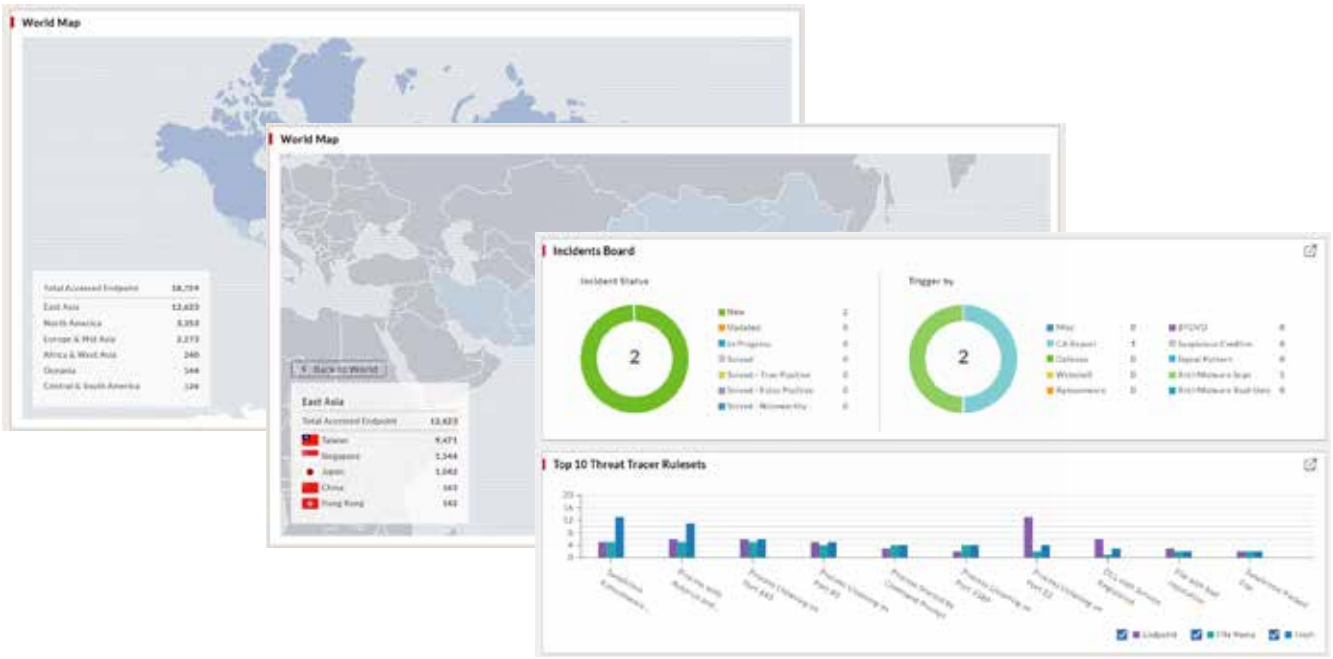
- **多層防御** – アンチランサムウェアとアンチマルウェアを組み合わせた統合型EDRプラットフォームにより多層的な防御を実現します。
- **自己学習エンジンによる脅威識別** – エンジンの自己学習機能により一般的に使用されるアプリケーションや新たに出現するマルウェアを識別します。
- **振る舞いベースの防御** – 高度な挙動分析により、検知精度を向上させ、誤検知を低減します。
- **リアルタイムのランサムウェア防御** – 継続的な監視により暗号化型ランサムウェア攻撃をブロックし、バックアップデータを保護します。

自動化防御と能動的な脅威ハンティング

- **デュアル検知エンジン** – エンドポイント全体で悪意のあるファイルや不審な挙動を検知します。
- **自動化された脅威防止** – 既知の脅威を迅速に封じ込め、攻撃を阻止します。
- **能動的な脅威ハンティング** – 未知または新たに出現する攻撃手法を特定・調査します。

高効率で柔軟な導入

- **軽量シングルエージェント** – システムへの影響を最小限に抑えながら迅速な導入を実現します。
- **脅威インテリジェンスの自動更新** – マルウェアデータベースを継続的に更新し、運用を中断することなく最新の脅威情報を維持します。
- **柔軟な導入オプション** – クラウド環境とオンプレミス環境の両方に対応し、組織の運用環境にあわせた導入が可能です。



機能

MITRE ATT&CK®に基づく脅威分析

攻撃活動をMITRE ATT&CKに自動的にマッピングし、攻撃者のTTP（戦術・技術・手順）を可視化するとともに、既知の脅威グループに対するセキュリティ対策の有効性を検証します。

攻撃チェーンの可視化

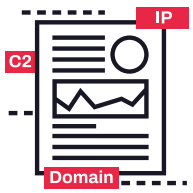
グラフベースの攻撃経路分析は、侵入経路や攻撃行動を明確に可視化し、インシデントの調査と対応を迅速化します。

タイムラインベースのインシデント分析

イベントやエンドポイントのタイムラインにより攻撃の一連の流れを再構成し、インシデント分析やフォレンジック調査を迅速化します。

ThreatSonarによる包括的なランサムウェア防御

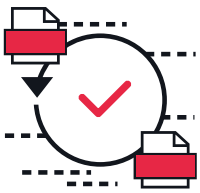
侵害前 防御 → 侵害発生 検知 → 侵害後 対応



脅威インテリジェンス
将来の攻撃の予測

エンドポイント
ランサムウェアの阻止

リアルタイム対応
脅威の拡散を阻止



復旧
バックアップデータの保護

TeamT5 について

世界中の550社を超えるクライアントに信頼をいただき、政府機関、テクノロジー、金融、医療、軍事、通信など幅広い業界にサービスを提供しております。

トップレベルのサイバーセキュリティ専門家

TeamT5のメンバーは、Black Hat（米国）、JCode Blue／AVTokyo（日本）、Troopers（ドイツ）などの世界的なサイバーセキュリティカンファレンスをはじめ、Hack In The Box や FIRST などの国際的なセキュリティコミュニティにおいて、最先端の研究成果を頻繁に発表しています。脅威インテリジェンス研究および高度なサイバーセキュリティ技術の分野で、世界トップクラスの実績を有しています。

メディア掲載・業界評価

TeamT5は、Bloomberg、CNN、The Wall Street Journal、Reuters、The Guardian、WIRED、NHKなどの国際的なメディアから、サイバーセキュリティ分野の専門家として取材を受けるだけでなく、日本最大級のベンチャーキャピタルであるJAFCO Asia、日本を代表する総合商社の伊藤忠商事、国内有数のサイバーセキュリティサービスプロバイダーであるマクニカなどからも高い評価と支援を受けています。

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

v.202605

TEAMT5 | THREAT INTELLIGENCE PIONEER, BORN IN ASIA