Datasheet

ThreatSonar

TEAMT5

ThreatSonar Plus

統合型エンドポイントリスク評価プラットフォーム

重要なリスクを明らかにし、セキュリティ侵害を未然に防止

AIエージェントがエンドポイントにおいてデータアクセスやコマンド実行の能力を持つようになったことで、セキュリティの境界は変化しました。自動化攻撃が頻発する中、企業のリスクはもはやシステムの脆弱性にとどまらず、AIエージェントの権限利用や挙動にまで広がっています。企業には、エンドポイントとAIエージェント双方がもたらすリスクを統合的に管理するための体系的な評価が求められています。

単一の評価でエンドポイントとAIエージェントのリスクを把握

ThreatSonar Plusは「資産インベントリ」と「リスク検知」に基づいて構築された包括的なリスク評価プラットフォームであり、単一の評価によってエンドポイント資産およびAIエージェントの利用状況を把握できます。

本プラットフォームは、システム、ソフトウェア、アプリケーション、およびAIエージェントを識別し、データアクセス、コマンド実行、権限設定などのリスクを分析します。さらに、脆弱性インテリジェンス、リスクスコアリング、資産の重要度を組み合わせることで、対応の優先順位付けを支援します。

利点

- **優先順位付けされた対応により、重要なリスクをより迅速に特定**
  エンドポイントとAIエージェントのリスクをカバーする統合的な評価手法
- **修復対応を迅速化し、リスクの露出期間を短縮**
  脆弱性を追跡し、ゼロデイリスクを低減するためのガイダンスを提供
- **国際標準に基づく設定強化**
  CISベンチマークに基づきシステム設定を評価し、具体的な改善指針を提供
- **SEMI E187への対応**
  E187の各領域に対する自動評価と明確なレポート

4つの簡単なステップでリスクを評価

どのような資産が存在するのか？	どのようなリスクが既に存在するか？	どのリスクを優先すべきか？	どのようにリスクに対応するか？
資産インベントリ 環境内にどのようなエンドポイント機器、インストール済みソフトウェア、OS、AIエージェントの使用状況があるかを可視化する	**リスク特定** 脆弱性、設定ミス、AIエージェントに関する潜在的リスクを特定する	**リスクの優先順位付け** 深刻度に基づき、対応の優先順位を決定する	**対応判断** リスクに関する情報と是正ガイダンスを提供し、その後の対応および意思決定を支援する

主な特徴

AIエージェントに対する多面的なリスク評価

ThreatSonar Plusは、AIエージェントによってもたらされるリスクを特定し、機密データの保護から悪意あるコマンド追跡までの包括的な防御を提供します。

機密データ保護

APIキー、認証情報、機密データの保存場所を自動的に識別し、タスク実行時にコア資産を誤用または漏えいといった、AIエージェントによる露出リスクを低減します。

悪意あるスキルの検知

サードパーティのAIスキルを深く分析し、隠れたバックドアや悪意ある挙動を正確に識別し、自動化ツールチェーンの安全性とコンプライアンスを確保します。

隠しコマンドの分析

AIが生成するシステムコマンドをリアルタイムで監視し、潜在的な悪意ある挙動やコマンドインジェクションを検出することで、自動化攻撃の足がかりを防ぎます。

最小権限制御

AIエージェントのアクセス範囲を評価・制限し、最小権限の原則を厳格に遵守することで、セキュリティ管理の盲点を排除します。

SEMI E187準拠評価

ThreatSonar Plusの自動リスク評価は、SEMI E187の4つの各領域（OS規範、ネットワークセキュリティ、エンドポイント保護、情報セキュリティ監視）を網羅しています。OSがサポート対象かどうかを確認し、ネットワークプロトコル（HTTPS、SFTPなど）やポート設定の安全性を評価します。
検査結果に基づき、標準化されたレポートとリスクサマリーを自動生成し、組織が迅速に脆弱性を発見・修復できるようにすることで、SEMI E187 準拠を支援します。

機能

包括的な資産およびAIエージェントのインベントリ

資産インベントリはリスク評価の基盤であり、エンドポイント機器、OS、アプリケーションに加え、AIエージェントの展開と利用をカバーします。
これにより、資産の分布状況およびAIエージェントの利用状況を可視化し、その後のリスク分析および管理を支援します。

統合リスク検知と脅威分析

リスク検知はエンドポイントの脆弱性や設定、AIエージェントの利用状況をカバーし、潜在リスクを全面的に把握します。さらにAIエージェントの設定や挙動を分析し、リスクの露出を特定します。

資産情報はCPEにマッピングされ、CVEデータベースと照合されることで、完全な脆弱性情報とリスク評価を提供します。また、システム設定はCIS基準に基づき評価され、セキュリティベースラインへの準拠状況を検証します。

柔軟な導入と簡単な操作性

ThreatSonar Plusはオンラインとオフラインの両方の導入をサポートします。オンライン環境では結果を自動アップロードし、オフライン環境では手動で分析に取り込むことができます。インストール不要のポータブル版は外部デバイスから実行でき、検査対象にデータを残さず、安全かつ柔軟な運用を実現します。

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