

ThreatSonar Plus

包括的エンドポイントリスク 評価プラットフォーム

重要なリスクを把握し、セキュリティ脅威に早期対応

AIエージェントが企業のエンドポイントや業務プロセスへ急速に統合されるなか、セキュリティの境界は変化しています。自動化された攻撃も頻発し、企業が直面するリスクは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把握するための体系的な評価が求められています。

1回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

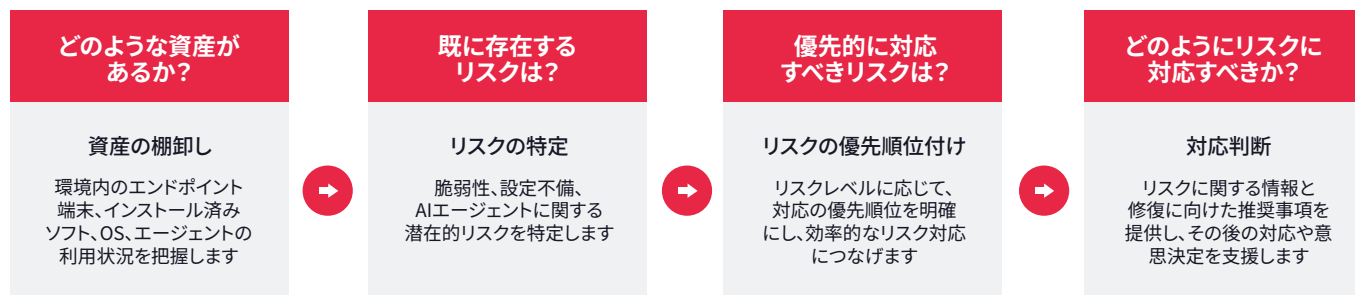
ThreatSonar Plusは「資産の棚卸し」と「リスク検知」を中核とする包括的なリスク評価プラットフォームです。1回の評価で、エンドポイント資産とAIエージェントの利用状況を包括的に棚卸しできます。

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、AIエージェントを識別し、データアクセス、コマンド実行、権限設定などの潜在的なリスクを分析します。さらに、脆弱性情報、リスクスコア、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、その後の改善、ガバナンス、監査に活用できる評価結果を提供します。

主な利点

- **重要なリスクを迅速に特定し、優先的に対応**
ワンストップの評価で、エンドポイントとAIエージェントのリスクを包括的に把握
- **修復を効率化し、脆弱性の露出期間を短縮**
実際の攻撃で悪用されている高リスクな脆弱性を照合し、優先的な修復につなげることで、攻撃リスクの低減を支援
- **国際標準に基づいてセキュリティ設定を強化**
CISベンチマークに基づきシステム設定を評価し、改善に向けた指針を提供
- **SEMI E187への適合性評価に対応**
SEMI E187の4つのセキュリティ領域を自動評価し、結果を分かりやすくレポート

4つの簡単なステップでリスクを評価



主な特徴

AIエージェントの多面的なリスク評価

ThreatSonar Plusは、AIエージェントがもたらす自動化された脅威に対応するため、信頼性の高いOWASPのAIエージェントのリスク分類に基づき、AIVSSスコアリングの仕組みを採用した包括的な検知・評価を行います。これにより、機密データの露出から悪意のあるスキルやコマンドまで、AIエージェントに関する潜在リスクの把握を支援します。

機密データの露出リスク

APIキー、認証情報、機密データの保存場所を一覧化し、エンドポイント上で露出する可能性のある機密情報を把握します。

悪意のあるスキルの識別

サードパーティ製およびオープンソースのスキルを識別し、その中にバックドアや悪意のあるコードが含まれている可能性、またマルウェアをダウンロードまたは実行するリスクを把握します。

隠されたコマンドの分析

AIエージェントに関連するツール説明や設定内容を解析し、隠されたコマンド、危険なコマンド、その他の不審な内容を特定します。

権限とアクセス範囲の評価

AIエージェントの権限とタスク範囲を確認し、タスクに必要な範囲を超えている可能性のあるアクセス設定を特定します。

SEMI E187への適合性評価

ThreatSonar Plusは、自動化されたリスク評価と適合性評価を提供し、SEMI E187の4つのセキュリティ要件である、OSに関する要件、ネットワークセキュリティ、エンドポイント保護、情報セキュリティモニタリングをカバーします。OSのサポート状況、ネットワークプロトコル、ポート、エンドポイント保護の設定を確認し、潜在的なリスクや規格に適合していない項目を迅速に特定します。

評価完了後は、評価結果と改善に向けた推奨事項をまとめた標準化された適合性評価レポートとリスクサマリーを自動生成します。これにより、手作業による確認コストを削減し、半導体製造装置メーカーが装置のセキュリティ状況を把握するとともに、SEMI E187への適合性評価や継続的な改善の根拠として活用できるよう支援します。

評価結果の概要

Item	Status
E187-00-RQ-00001-00	Pass
E187-00-RQ-00003-00	Pass
E187-00-RQ-00005-00	Fail
E187-00-RQ-00007-00	Pass
E187-00-RQ-00009-00	Pass
E187-00-RQ-00011-00	Pass
E187-00-RQ-00012-00	Pass

Device Information

Hostname	DESKTOP-1234567
OS	Windows 11 22H2
CPU	Intel Core i7-12700K
CPU Core Count	16
Total Memory Size	32 GB
Available Memory Size	16 GB
Install Time	2023-10-27 10:30:12 UTC
Time Zone	UTC+9:00

インストール済みソフト/アプリ一覧

Item	Status
E187-00-RQ-00001-00	Pass
E187-00-RQ-00003-00	Pass
E187-00-RQ-00005-00	Fail
E187-00-RQ-00007-00	Pass
E187-00-RQ-00009-00	Pass
E187-00-RQ-00011-00	Pass
E187-00-RQ-00012-00	Pass

Device Network Interfaces

Description	Intel(R) Wi-Fi 6E AX210
Default Gateway	192.168.1.1
IP Address	192.168.1.101
Network Mask	255.255.255.0
Mac Address	9C:5C:6D:15:2A:47

Scanner Information

Scanner Location	C:\Program Files\ThreatSonarPlus\Scanner\
Pattern Version	20231027
Module Version	20231027
Leader Version	20231027

Installed Applications

Name	Vendor	Version	File Path
Adobe Reader DC	Adobe Systems Inc.	20.005.20005	C:\Program Files\Adobe\Adobe Reader\
Adobe Reader DC	Adobe Systems Inc.	20.005.20005	C:\Program Files\Adobe\Adobe Reader\
Adobe Reader DC	Adobe Systems Inc.	20.005.20005	C:\Program Files\Adobe\Adobe Reader\
Adobe Reader DC	Adobe Systems Inc.	20.005.20005	C:\Program Files\Adobe\Adobe Reader\

Windowsパッチ更新状況

Item	Name	Install Time
E187-00-RQ-00001-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00003-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00005-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00007-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00009-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00011-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00012-00	KB5026202	2023-10-27 10:30:12 UTC

E187ルール検知結果

Item	Name	Install Time
E187-00-RQ-00001-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00003-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00005-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00007-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00009-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00011-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00012-00	KB5026202	2023-10-27 10:30:12 UTC

重大な脆弱性と悪用状況

Item	Name	Install Time
E187-00-RQ-00001-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00003-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00005-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00007-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00009-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00011-00	KB5026202	2023-10-27 10:30:12 UTC
E187-00-RQ-00012-00	KB5026202	2023-10-27 10:30:12 UTC

Critical Vulnerabilities

Trigger by	CVE	Severity	Known Exploited
Adobe Acrobat Reader	CVE-2024-0001	High	Yes
Google Chrome	CVE-2024-0002	Medium	No
GitLab	CVE-2024-0003	Low	No

機能

資産を包括的に可視化し、AIエージェントの利用状況を把握

資産の棚卸しはリスク評価の基盤です。エンドポイント端末、OS、アプリケーションに加え、AIエージェントの導入状況や利用状況も対象とし、環境内の資産とAIエージェントの利用状況を包括的に可視化します。これらの情報を、その後のリスク分析や管理に活用できます。

多面的なリスク検知で、エンドポイントのリスクを可視化

リスク検知では、エンドポイントの脆弱性とAIエージェントの利用状況を対象とし、潜在的なリスクを包括的に把握します。さらに、AIエージェントのリスクについては、関連する設定内容を確認し、潜在的なリスクを分析します。

脆弱性検知では、資産情報をCPEに変換し、CVEデータベースと照合することで、包括的な脆弱性情報とリスク評価に必要な情報を提供します。また、セキュリティ設定については、CISベンチマークに基づきエンドポイント設定を確認し、セキュリティベースラインへの適合状況を確認します。

柔軟な導入方式で、多様な環境に対応

ThreatSonar Plusは、オンラインとオフラインの両方の導入方式に対応しています。ネットワーク接続環境では、評価完了後に結果を自動アップロードし、オフライン環境では手動で結果をインポートして分析できます。

また、インストール不要版も提供しており、ポータブルデバイスから評価を実行できます。評価対象端末上にデータを生成せず、環境設定も変更しないため、安全性と操作性を両立できます。

TeamT5 について

v.202609

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セキュリティ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。