



# ThreatSonar Plus

## Extensive Endpoint Assessment Platform

### Uncover Critical Risks. Stop Breaches.

As AI agents are rapidly integrated into enterprise endpoints and workflows, the security boundary has changed. Beyond vulnerabilities, organizations now face automated threats targeting AI agent behaviors and permissions. Organizations need systematic assessment to control over the overall risks posed by both endpoints and AI agents.

### Identify Endpoint and AI Agent Risks in One Assessment

ThreatSonar Plus is a comprehensive risk assessment platform built on Asset Inventory and Risk Detection, enabling organizations to perform a one-time assessment to inventory endpoint assets and AI agent usage.

The platform identifies systems, software, applications, and AI agents, and analyzes risks such as data access, command execution, and permission configurations. By combining vulnerability intelligence, risk scoring, and asset criticality, it supports remediation prioritization and provides assessment results for follow-up improvement, governance, and audit.

#### Benefits

- **Spot critical risks faster with prioritized remediation**  
A unified assessment approach covering endpoint and AI agent risks.
- **Accelerate remediation to shrink exposure windows**  
Identify high-risk vulnerabilities exploited in the wild and patch them early to reduce attack risk.
- **Harden configurations with global standards**  
CIS benchmarking with actionable hardening guidance.
- **Support needs of SEMI E187 compliance**  
Automated assessment across E187 domains with clear reporting.

### Assess Risks in 4 Simple Steps



### Key Highlights

#### Multi-dimensional AI Agent Risk Assessment

ThreatSonar Plus addresses automated threats introduced by AI agents with comprehensive detection and assessment based on the widely recognized OWASP Agentic AI risk taxonomy and its AIVSS scoring framework, helping organizations identify potential risks ranging from sensitive data exposure to malicious skills and commands.

##### Sensitive data exposure

Lists API keys, credentials, and sensitive-data storage locations to identify potentially exposed sensitive information on endpoints.

##### Malicious skill identification

Identifies third-party and open-source skills that may contain hidden backdoors or malicious code, or pose risks of downloading or executing malware.

##### Hidden command analysis

Analyzes AI-agent tool descriptions and configuration content to identify hidden commands, dangerous commands, or other suspicious content.

##### Permission and access scope assessment

Reviews AI-agent permissions and task scope to identify access settings that may exceed what the task requires.

## SEMI E187 Compliance Assessment

ThreatSonar Plus provides automated risk and compliance assessment across the four SEMI E187 security domains: operating system security, network security, endpoint protection, and security monitoring. It checks OS support status, network protocols and ports, and endpoint protection settings to quickly identify potential risks and non-compliant items.

After assessment, ThreatSonar Plus automatically generates standardized compliance reports and risk summaries with findings and improvement recommendations. This reduces manual validation effort and helps semiconductor equipment vendors understand equipment security status for SEMI E187 compliance assessment and continuous improvement.

### Assessment Results Overview

**Overview**

| Scan Status         | Result |
|---------------------|--------|
| 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 | Fail   |
| E187-00-RQ-00010-00 | Pass   |
| E187-00-RQ-00011-00 | Pass   |
| E187-00-RQ-00012-00 | Pass   |

**Device Information**

|                       |                          |
|-----------------------|--------------------------|
| Hostname              | DPT-F101 Windows Desktop |
| OS                    | Windows 11 24H2          |
| CPU                   | Common KRM processor     |
| CPU Core Count        | 6                        |
| Total Memory Size     | 8192 MB                  |
| Available Memory Size | 1885 MB                  |
| Install Time          | 2020-09-22 10:20:12 UTC  |
| Time Zone             | UTC+08:00                |

### Installed Software and Application Inventory

**Device Network Interfaces**

|                 |                      |
|-----------------|----------------------|
| Description     | Intel(R) PRO/1000 MT |
| Default Gateway | 192.168.2.254        |
| IP Address      | 192.168.2.254        |
| Network Mask    | 255.255.255.0        |
| Mac Address     | 96-29-47-15-28-17    |

**Scanner Information**

|                  |                                           |
|------------------|-------------------------------------------|
| Scanner Location | C:\Program Files\ThreatSonarPlus\Scanner\ |
| Pattern Version  | 2501p0                                    |
| Module Version   | 2501p0                                    |
| Loader Version   | 2501p0                                    |

**Installed Applications**

| Name            | Vendor             | Version      | File Path                                                                  |
|-----------------|--------------------|--------------|----------------------------------------------------------------------------|
| Adobe Reader DC | Adobe Systems Inc. | 21.003.20035 | C:\Program Files (x86)\Adobe\Reader\Acrobat Reader DC\Reader\Acrobat21.exe |
| Adobe Reader DC | Adobe Systems Inc. | 21.003.20035 | C:\Program Files (x86)\Adobe\Reader\Acrobat Reader DC\Reader\Acrobat21.exe |
| Adobe Reader DC | Adobe Systems Inc. | 21.003.20035 | C:\Program Files (x86)\Adobe\Reader\Acrobat Reader DC\Reader\Acrobat21.exe |
| Adobe Reader DC | Adobe Systems Inc. | 21.003.20035 | C:\Program Files (x86)\Adobe\Reader\Acrobat Reader DC\Reader\Acrobat21.exe |

### Windows Patch Updates

**Updated Windows Patches**

| Item      | Name                                       | Install Time               |
|-----------|--------------------------------------------|----------------------------|
| KB5034423 | Security for Microsoft Windows (KB5034423) | 2024-09-23 17:28:12 +08:00 |
| KB5034423 | Security for Microsoft Windows (KB5034423) | 2024-09-23 17:28:12 +08:00 |

**E187-00-RQ-00003-00**

**Port Settings**

| Port | Services     | Status |
|------|--------------|--------|
| 21   | TFTP (tftpd) | Pass   |
| 21   | TFTP (tftpd) | Pass   |
| 21   | SNMP (snmp)  | Pass   |
| 21   | HTTP         | Fail   |
| 21   | HTTPS        | Pass   |

**Rules Check**

| Rule                | Status |
|---------------------|--------|
| E187-00-RQ-00003-00 | Pass   |
| E187-00-RQ-00003-00 | Pass   |

### Critical Vulnerabilities and Exploitation Status

**E187-00-RQ-00005-00**

| Critical | High | Medium | Low |
|----------|------|--------|-----|
| 40       | 989  | 512    | 89  |

**Critical Vulnerabilities**

Trigger by: Adobe Acrobat Reader

| Vulnerability | CVE | Published Date          | Known Exploited |
|---------------|-----|-------------------------|-----------------|
| CVE-2024-4371 | 10  | 2024-09-25 17:28:12 UTC | False           |
| CVE-2024-4371 | 10  | 2024-09-25 17:28:12 UTC | False           |

Trigger by: Google Chrome

| Vulnerability | CVE | Published Date          | Known Exploited |
|---------------|-----|-------------------------|-----------------|
| CVE-2024-4371 | 10  | 2024-09-25 17:28:12 UTC | False           |
| CVE-2024-4371 | 10  | 2024-09-25 17:28:12 UTC | True            |
| CVE-2024-4371 | 10  | 2024-09-25 17:28:12 UTC | False           |

Trigger by: GitLab

| Vulnerability | CVE | Published Date          | Known Exploited |
|---------------|-----|-------------------------|-----------------|
| CVE-2024-4371 | 10  | 2024-09-25 17:28:12 UTC | True            |

**E187-00-RQ-00007-00**

| Rule                | Status |
|---------------------|--------|
| E187-00-RQ-00007-00 | Pass   |

## E187 Rules Detection

## Capabilities

### Comprehensive Asset Visibility and AI Agent Usage

Asset inventory forms the foundation of risk assessment, covering endpoints, operating systems, applications, as well as AI agent deployment and usage. It provides full visibility into asset distribution and AI agent usage, supporting subsequent risk analysis and management.

### Multi-dimensional Risk Detection and Endpoint Risk Visibility

Risk detection covers endpoint vulnerabilities, endpoint configurations, and AI agent usage, providing a comprehensive view of potential risks. AI-agent settings are reviewed to identify potential risks.

Assets are mapped to CPEs and correlated with CVE databases to deliver complete vulnerability insights and risk references, while system settings are assessed against CIS benchmarks to verify security baseline compliance.

### Flexible Deployment Across Diverse Environments

ThreatSonar Plus supports both online and offline deployment. Connected systems automatically upload results after assessment, while offline systems allow manual import for analysis. A portable, installation-free version runs from removable devices without leaving data on the assessed device or changing environment settings, ensuring secure, flexible operation.

## About TeamT5

v.202609

Widely trusted by more than 550 customers around the world, including government departments, technology, manufacturing, finance, medical care, military, telecommunications and other industries.

TeamT5 has more than 20 years of experiences in malware and advanced persistent penetration attacks (APT). With language and cultural advantages, we possess specific expertise in cyber espionage in the Asia-Pacific region, and are often invited to present the latest information at world-class cybersecurity conferences, including Black Hat in the United States, Code Blue / AVTokyo in Japan, Troopers in Germany, and Hack In The Box and FIRST. As a world-leading team in the field of threat intelligence research and advanced cybersecurity technology, we have also been interviewed by Bloomberg and CNN in the United States, Sankei Shimbun and Asahi Shimbun in Japan, and ET News in South Korea.