Datasheet

ThreatSonar

TEAMT5

ThreatSonar Plus

Extensive Endpoint Assessment Platform

Uncover Critical Risks. Stop Breaches.

As AI agents enable endpoints to access data and execute commands, 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 prioritization of remediation.

Benefits

- **Spot critical risks faster with prioritized remediation**
  A unified assessment approach covering endpoint and AI agent risks.
- **Accelerate remediation to shrink exposure windows**
  Track vulnerabilities and provide guidance to reduce zero-day risks.
- **Harden configurations with global standards**
  CIS benchmarking with actionable hardening guidance.
- **Achieve compliance with SEMI E187**
  Automated assessment across E187 domains with clear reporting.

Assess Risks in 4 Simple Steps

What assets are present?	What risks already exist?	Which risks require priority attention?	How can risks be addressed?
Asset Inventory Gain visibility into endpoint devices, installed software, operating systems, and AI agent usage.	**Risk Identification** Identify vulnerabilities, misconfigurations, and AI agent risks.	**Risk Prioritization** Determine remediation priorities based on severity.	**Response Decision** Provide risk insights and remediation guidance for follow-up actions.

Key Highlights

Multi-dimensional AI Agent Risk Assessment

ThreatSonar Plus identifies risks introduced by AI agents, providing protection from sensitive data exposure to malicious command execution.

Sensitive data protection

Automatically identify API keys, credentials, and sensitive data locations to reduce exposure risks.

Malicious skill detection

Analyze third-party AI skills to pinpoint hidden backdoors and malicious actions, ensuring toolchain security and compliance.

Hidden command analysis

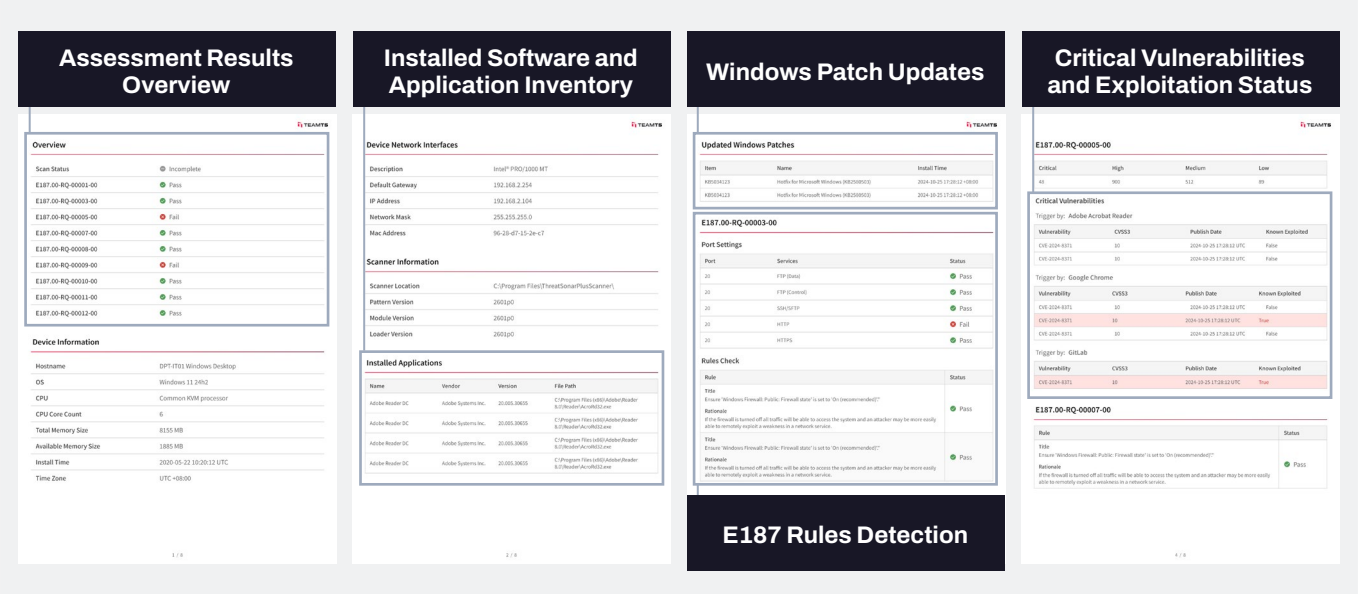
Monitor AI-generated system commands to detect malicious behavior and injection risks, preventing automated attack footholds.

Least privilege control

Assess and restrict AI agent access to enforce least privilege and eliminate security control blind spots.

SEMI E187 Compliance Assessment

ThreatSonar Plus supports automated assessment aligned with SEMI E187, covering operating systems, network security, endpoint protection, and security monitoring. It verifies OS support status and evaluates secure protocols (e.g., HTTPS, SFTP) and port configurations. Standardized reports and risk summaries help organizations identify and remediate, achieving compliance.



Capabilities

Comprehensive Asset and AI Agent Inventory

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.

Integrated Risk Detection and Threat Analysis

Risk detection covers endpoint vulnerabilities, endpoint configurations, and AI agent usage, providing a comprehensive view of potential risks. AI agent configurations and behaviors are analyzed to identify exposures.

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 and Ease of Use

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, leaving no data on the assessed device and ensuring secure, flexible operation.

About TeamT5

v.202605

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.

Tel +886-2-7706-1299
E-mail sales@teamt5.org

TEAMT5 | THREAT INTELLIGENCE PIONEER, BORN IN ASIA