ThreatVISION

Threat Hunting Tools: A Powerful Asset for Proactive Defense

Intelligence-Driven Proactive Defense Tools

ThreatVision provides ready-to-use threat hunting tools to help organizations quickly spot potential threats and strengthen security processes. Developed by TeamT5 analysts, these tools uncover attacker tools, backdoors, and operational traces.

The Best Solution for Cybersecurity Pain Points

Covers Multiple Variants and Sample Types	Detection rules (like YARA, Sigma) cover malware variants, identifying a wide range of attack behaviors.
Curated Rules to Reduce Analysis Burden	Pre-filter low-relevance logs and alerts, letting analysts focus on anomalies and cut false positives.
Correlated Intelligence to Build Attack Context	Provide related adversaries, samples, and TTPs to assess impact and prioritize response.
Deployable on Existing Systems	Tools can be imported into SIEM & TIP, speeding up threat hunting even with limited resources.

One-Click Download for Required Tools

Tools are categorized by target (malware, vulnerabilities) and type (YARA, Snort, Sigma), sorted by release date for easy one-click download, available right from the platform' s homepage.

Benefits

Quickly Grasp the Threat Landscape

Understand potential threats & anomalies to facilitate response.

Enhance Detection of Unknown Attacks

Strengthen malware variants & attacks detection with updated rules.

Integrate into Automated Processes

Standardized YARA, Snort, Sigma rules for existing systems & workflows.

Improve Vulnerability Response

Prioritize patching exploited vulnerabilities of at-risk systems & assets.

Expand Defense Coverage

Detect malware & vulnerability exploits for stronger proactive defense.

Applicable Roles

Security Teams

Implement threat hunting to strengthen detection & response.

SOC Analysts

Filter alerts, verify IoCs & improve investigation efficiency.

Incident Responders

Match samples and TTPs to establish attack context & attribution.

Security Engineers

Integrate rules into architectures to improve detection & automation.

Security Decision-Makers

Adjust patching & resources per detection results for strategic defense.

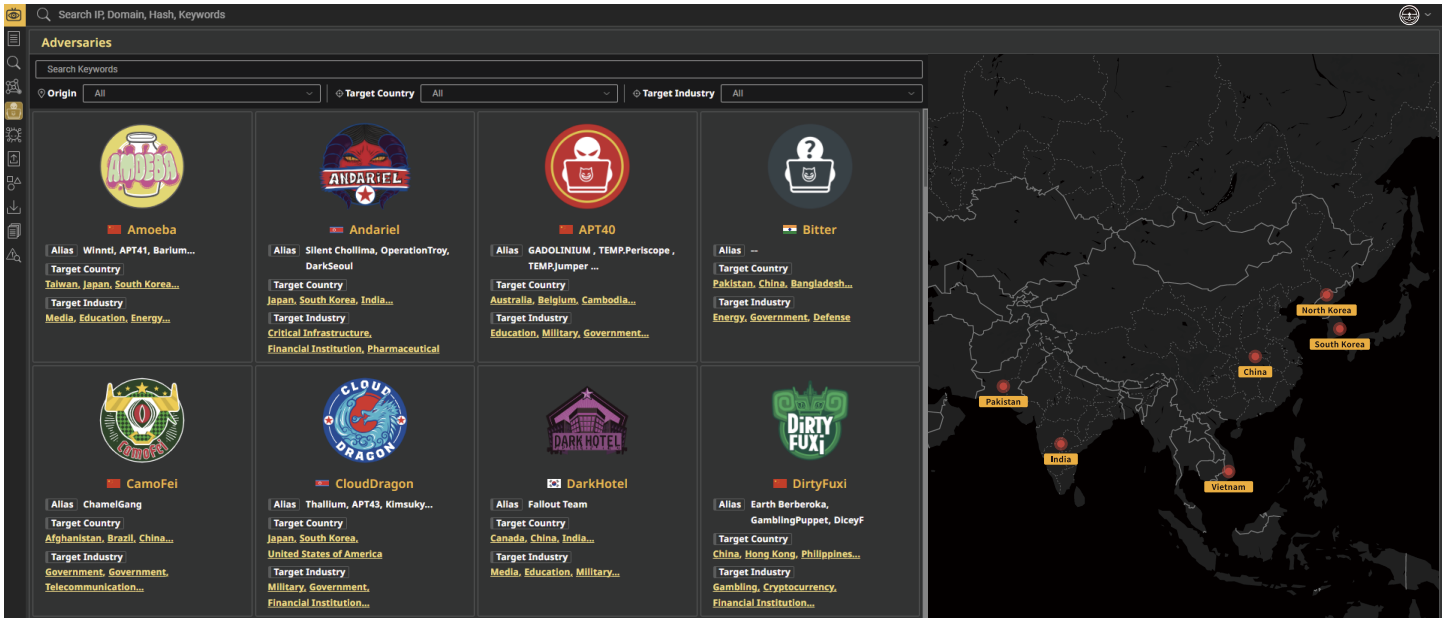
Diverse Application Scenarios

ThreatVision threat hunting tools cover various detection needs and scenarios, primarily divided into three categories:

Various Detection Rules	YARA, Snort, and Sigma rules enable rapid detection of file or behavioral anomalies on hosts or automated platforms.
Malware Hunting Tools	Detect high-risk malware (e.g., ShadowPAD) and its variants, complementing traditional antivirus coverage.
Vulnerability Detection Tools	Identify exploited vulnerabilities, assess impact scope, and detect related malicious programs.

ThreatVision Platform Overview

ThreatVision' s diverse intelligence supports various roles and tasks, helping organizations fully grasp the behavioral patterns of adversaries and proactively deploy defensive strategies. It is the optimal solution from strategic planning to frontline defense.



Get Started with ThreatVision

Please contact the TeamT5 sales team to request a 14-day trial account for ThreatVision. For further information, please email sales@teamt5.org. We look forward to helping protect your organization from cyber threats.

About TeamT5

Trusted by over 300 clients worldwide, spanning industries such as government, technology, manufacturing, finance, medical, military, and telecommunications.

A Team of Leading Experts

Our team members are world leaders in threat intelligence research and advanced security technology, frequently presenting their latest research at world-class cybersecurity conferences. These include HITCON (Taiwan), Black Hat (USA), Code Blue/AVTOKYO (Japan), Troopers (Germany), as well as international events organized by Hack In The Box and FIRST.

Industry Recognition

TeamT5 has been featured in interviews and reports by media outlets such as Bloomberg and CNN in the United States, Sankei Shimbun and Asahi Shimbun in Japan, and ET News in Korea. In 2022, the company received investment from three Japanese industry giants: JAFCO, Japan's largest venture capital group; ITOCHU, Japan's largest multinational corporation with global business investments; and MACNICA, Japan's largest cybersecurity solutions provider.

TeamT5 | Tel +886-2-7706-1299 | E-mail sales@teamt5.org

Website Facebook YouTube