



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	Curated Rules to Reduce Analysis Burden	Correlated Intelligence to Build Attack Context	Deployable on Existing Systems
Detection rules (like YARA, Sigma) cover malware variants, identifying a wide range of attack behaviors.	Pre-filter low-relevance logs and alerts, letting analysts focus on anomalies and cut false positives.	Provide related adversaries, samples, and TTPs to assess impact and prioritize response.	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.	

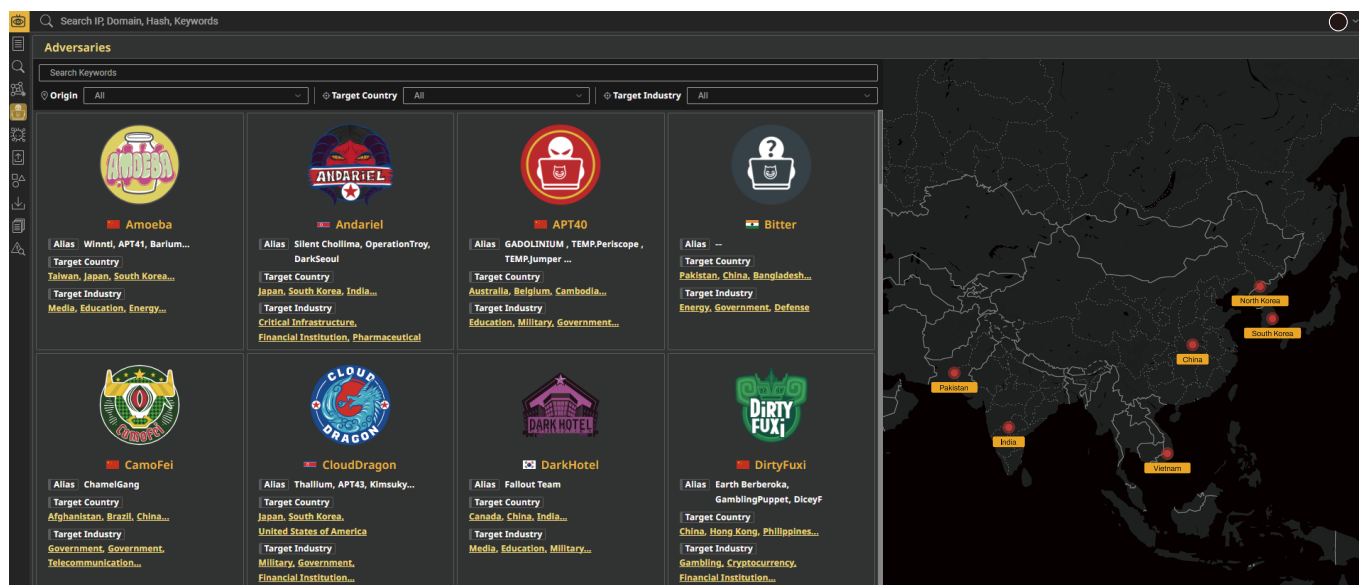
// Diverse Application Scenarios

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

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.