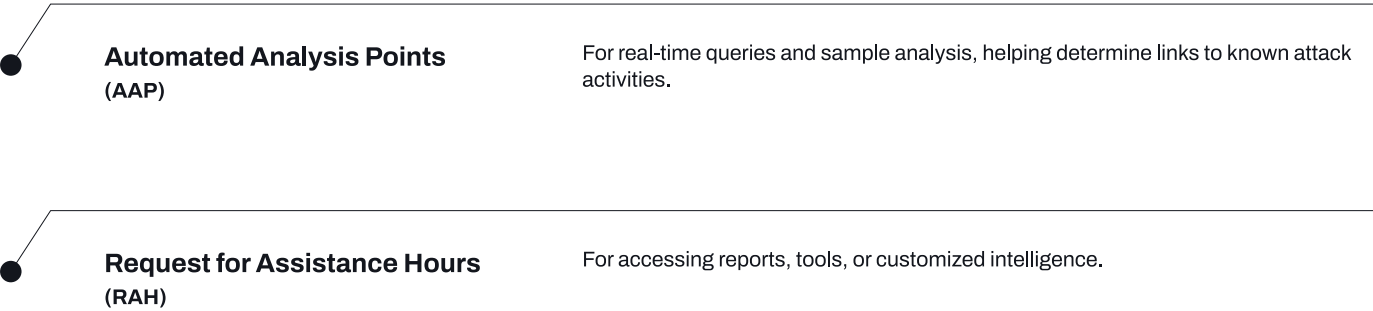




# Threat Intelligence Points: Maximizing the Value of Intelligence

To meet varying security needs, ThreatVision offers two point mechanisms, covering everything from real-time queries to advanced analysis:



## // ThreatVision Automated Analysis Points (AAP)

AAP enables fast, real-time queries to detect threats early. Common uses include alert triage, Indicator of Compromise (IoC) verification, and sample analysis.

**Use AAP For:**

| IP/Domain/Sample Queries                                                                   | Raw Intel Access                                                                    | Suspicious Sample Analysis                                                                |
|--------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Cross-check suspicious IPs/ domains/hashes with related adversaries, malware, and reports. | Retrieve unpublished observations (e.g. attacker activity, IoCs) for early warning. | Upload files for automated analysis of malicious programs to support triage and response. |

**Notes:**

- Points are prepaid and can be purchased as needed.
- Deductions are shown before executing sample analysis.
- Ideal for rapid-response scenarios like alert classification and sample detection.

## // ThreatVision Request for Assistance Hours (RAH)

RAH provides advanced support, covering access to specific report types, tool downloads, and customized intelligence services. It is especially useful for in-depth investigations of particular attacks or threat trends.

Use RAH For:

| Report Access                                                        | Threat Hunting Tools                                                                                   | Customized Intelligence Requests (RFI)                                                                   |
|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Unlock previously published reports, depending on subscription type. | Download YARA, Snort, and Sigma rules that can be deployed directly for faster detection and tracking. | Request tailored research with TeamT5's dedicated findings on industries, regions, or attack activities. |

Notes:

- Points are prepaid, with required points displayed in advance.
- Usage history available for management and auditing.
- Best suited for background investigation, attribution, and campaign analysis.

## // How to Choose Between AAP and RAH

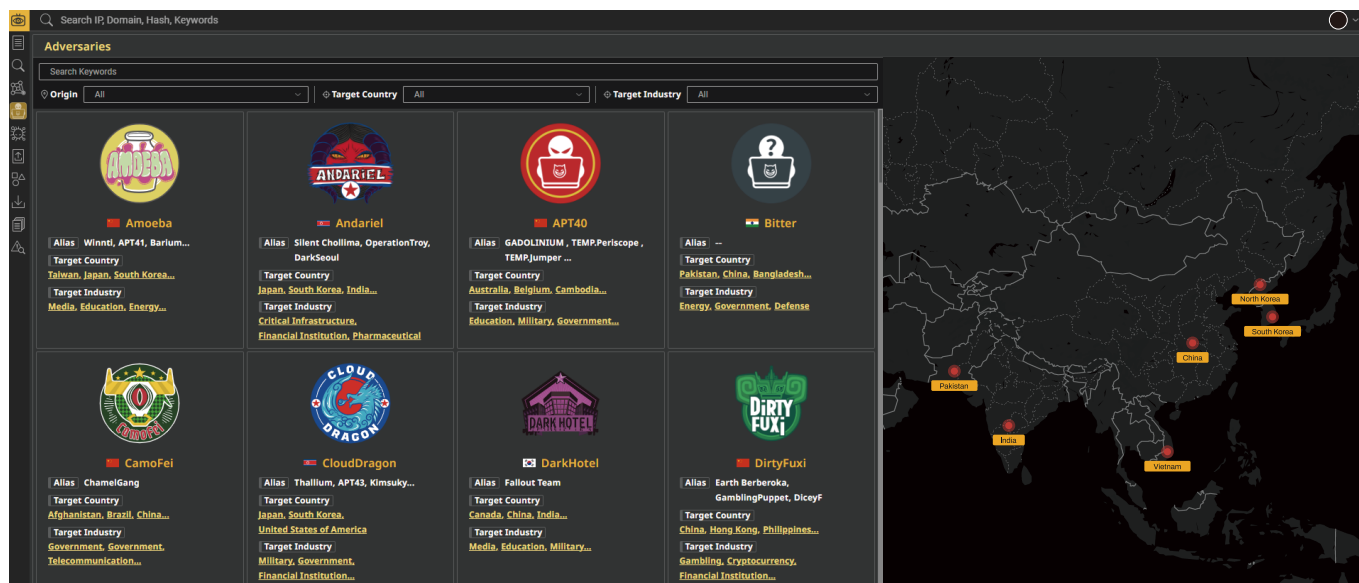
| AAP                                                                                                                                                                                                                                 | RAH                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>▪ Query suspicious IPs/domains to check for malicious activity.</li><li>▪ Upload samples for automated analysis.</li><li>▪ Access raw intel to assess exposure to emerging threats.</li></ul> | <ul style="list-style-type: none"><li>▪ Access specific reports and threat hunting tools.</li><li>▪ Submit customization requests on specific topics.</li><li>▪ Conduct analysis of attack techniques and campaigns.</li></ul> |

## // Immediate Activation for Maximum Intelligence Value

Whether you are an incident responder, SOC analyst, or CISO requiring rapid risk evaluation, AAP and RAH provide flexible options. Contact TeamT5 sales team for deployment guidance.

# 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](mailto: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.