

Indicators of Compromise: Precise Identification to Block Threats

The Challenges for Security Teams

Security teams are overwhelmed by high-volume alerts, leading to increased investigation costs, wasted resources, and missed breaches. Relying on external services is often too slow and expensive for a sustainable defense. ThreatVision's high-fidelity Indicators of Compromise (IoCs) solve this by increasing detection accuracy and response efficiency without burdening security teams, enabling a continuously effective defense.

5 Key Features

- Cross-scenario IoC application
- High-fidelity data sources
- Precise alert triggering
- Correlated intelligence integration
- Automated integration

4 Key Benefits

- Reduce false positives and alert fatigue
- Link threats to sources and attack context
- Support proactive threat detection and tracking
- Enable rapid deployment to strengthen defenses

What Makes ThreatVision's IoCs Different?

Built on TeamT5's long-term tracking of APAC threats, our Advanced Persistent Threat (APT) and Cybercrime (CC) IoCs transform firsthand observations into indicators rich with exclusive behavioral context. These analyst-verified IoCs integrate directly into your existing defenses, significantly improving alert triage and accelerating incident response. Users can query any indicator to get a comprehensive view of the associated attack, malware, and adversary, allowing them to take swift, informed action and strengthen their overall defense.

Features of ThreatVision APT and CC IoCs

APT IoC	CC IoC
• Focus on state-sponsored or mission-oriented APT. • Provide complete context related to adversaries, malware, and techniques. • Suitable for risk monitoring and analysis in highly sensitive industries (e.g., government and defense). • Release once per week, total 52 per year.	• Cover large-scale, non-targeted cybercrime activities. • Applicable for detecting ransomware, phishing, and credential theft, etc. • Improve alert quality and strengthen defense against high-frequency attacks. • Release once per week, total 52 per year.

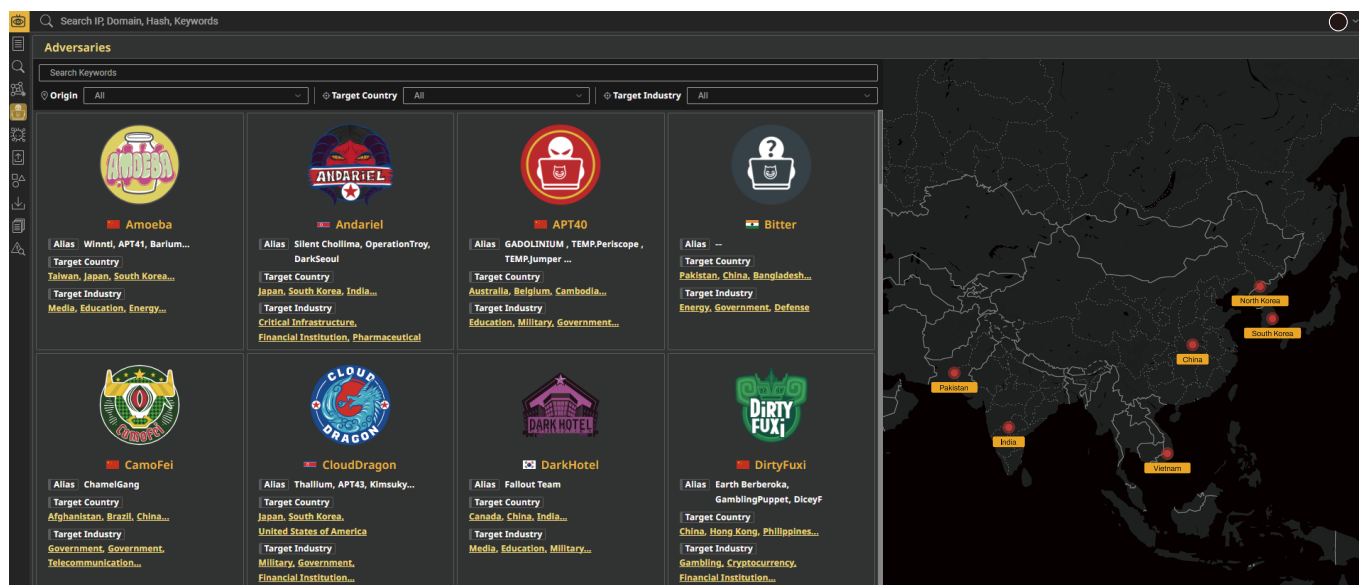
Note | During APT investigations, cybercrime-related intelligence may be uncovered. However, the IoC classification is based on whether an incident is identified as an APT attack, not the cybercrime type.

// Diverse Applications of ThreatVision IoCs

Organizational Needs	Application Examples
Needs coverage of multiple threat sources for effective detection.	A high-tech manufacturer applied APT & CC IoCs with tailored logic, improving alert accuracy and efficiency.
Needs trusted indicators to improve threat awareness.	A government agency used APT IoCs to monitor a nation-state actor, ensuring traceable intelligence for risk analysis.
Needs higher alert accuracy for real-time defense.	A financial services provider used CC IoCs to detect anomalous logins, reducing data breach risk.
Needs automated feeds to boost defensive efficiency.	A large enterprise fed IoCs into its SIEM via API, enabling real-time updates and reducing manual effort.
Needs faster incident investigations with attack context.	An incident responder queried IoCs in ThreatVision to obtain malware and adversary data, quickly building context.
Needs standardized formats for easier integration.	An MSSP ingested IoCs in STIX and CSV, enabling rapid client deployment and automated reporting.

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.