ThreatSonar

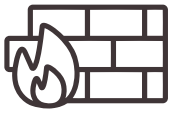
Threat Forensic Analysis Platform

Intelligence-driven Threat Forensics to Detect APT Attacks

APT (Advanced Persistent Threats) attack methods are ever-changing from day to day. Often when the attack is discovered, the important sensitive data of the enterprise has already been accessed by hackers. Therefore, early detection of threat attacks and reducing the time of lateral movement has become the primary issue of threat forensics.

Anti-hacking as Anti-epidemic
Proactively Hunts Hidden APT Threats with Intelligence

Anti-hacking is like epidemic prevention. Enterprises, government organizations take various measures to prevent threats and attacks, such as using firewalls for external block, installing anti-virus software for passive self-protection, just like controlling borders and wearing masks to prevent the spread of the epidemic. However, whether the information environment of enterprises, government and organizations is safe or not still needs to be confirmed through quick forensics.

Defensive measures	External prevention	Self protection	Verify safety
Defense against epidemic	Border control & quarantine	Wearing a mask / social distancing	Rapid test
			
	VS	VS	VS
Defense against cybersecurity threats			 ThreatSonar
	Firewall, IPS, WAF	Endpoint protection	

TeamT5 team, which has been researching global threat intelligence and tracking malicious programs for a long time, is well aware of the cybersecurity threat defense needs of enterprises, governments, and organizations. By using the exclusive APT risk model trained by threat behavior analysis, forward-looking technology and real cases, TeamT5 develops ThreatSonar Threat Forensic Analysis Platform, which can quickly check and verify the cybersecurity, and truly uncover hidden intrusion threats.

Key Benefits

Detected	Adopted	Implemented
1,000+	90%	1 million+
Successfully detected 1,000+ APT attacks that other competitors couldn' t find	Adopted by over 90% Managed Security Services Providers in Taiwan	Implemented 1 million+ endpoints forensics

- **Flexible deployment:**
  on-premises and cloud management mechanisms and compatible with multiple virtual structures.
- **Actively discovers hidden threats often used by hacker groups:**
  backed by global threat intelligence research, which accurately identifies malicious processes, early detects intrusion attacks and prevents unknown attacks.
- **Quick and Efficient Forensic:**
  Large-scale forensic (over 5,000 endpoints) can be done in an hour with sufficient hardware resources.
- **Shorten detection and response time:**
  auto-investigation analyzes hidden infections with similar TTPs and speeds up incident response execution.
- **OS Support:**
  Windows, Linux & MacOS

How does ThreatSonar Threat Forensic Analysis Platform Work?

Data Collection and Analysis

Advanced threat hunting technology finds out suspicious programs and file activities on endpoints, and finds out potential threats.

Intelligence-driven Forensics

Validate identified events through IOC, threat intelligence correlation.

Root Causes Analysis

Determines how the incident occurred and identifies threats.

Forensics Report

Includes identified threats and root causes. All activities during the forensics process are documented for future reference.

Industry-leading Features

Intelligence-driven smart threat forensics

Built-in thousands of APT backdoor signatures provide the latest intelligence to every endpoint for threat forensics. Also it allows to import external intelligence such as hash, IP, domain, Yara Rule and IoC to precisely defend potential targeted threats.

Lightweight deployment and background execution without affecting daily operations

ThreatSonar agent can be deployed on thousands of computers in an enterprise, and runs with less system resources. Personnel can carry out computer work as usual without the burden of running forensic.

Compromise assessment offers the whole picture of the incident, shortening the investigation time

ThreatSonar not only analyzes the current state of the host, but also investigates past event trajectories through log analysis, presents the sequence of events on the Timeline, and tracks lateral movement and data outflow paths through cross-endpoint correlation.

Possess memory forensics and behavior analysis to effectively identify unknown malicious programs

Identify malicious programs hidden in the memory, executed and to-be-executed programs, attacker's hacktools, and after-attacks log on the host, and automatically identify hundreds of dynamic behavior anomalies.

Active threat hunting with visualization of correlating potential compromised endpoints

Statistical correlation analysis finds unknown attack techniques, establishes baselines to lock on abnormal behaviors, and tags potential unknown threats, such as abuse of rare programs or legal system tools in the organization; malware with digital signatures, etc.

About TeamT5

Widely trusted by more than 300 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.

TeamT5 | Tel **02-7706-1299** | E-mail **sales@teamt5.org**