ThreatSonar ANTI-RANSOMWARE

# Endpoint Detection & Response

Cybersecurity teams in enterprises, government, and organizations face multiple challenges when detecting, investigating, and mitigating threat attacks. These teams need the corresponding analytical and investigative capabilities for the vast amount of data collected from various endpoints. Additionally, hacker attacks are often buried under a deluge of information, making it time-consuming for security personnel to identify genuinely suspicious behaviors. This hampers the progress of incident response and investigation and increasing operational costs.

## Intelligence-driven endpoint security enhances an organization's defense capabilities against threat attacks

TeamT5, which has conducted long-term research on global threat intelligence and tracked malicious programs, understands the cybersecurity defense needs of organizations. We have developed the ThreatSonar Anti-Ransomware Endpoint Detection & Response platform to stay ahead in continuous threat intelligence prediction and to monitor abnormal behaviors at all times. Upon detecting an attack, it issues immediate alerts, blocks malicious actions, and effectively responds to incidents, thereby reducing the damage.

## Benefits

- **Effective Cybersecurity Protection**
  High detection coverage, precise blocking of potential threats.
- **Reduced Response Time**
  Automatically analyze threats, expedite incident handling.
- **Alleviate Alert Fatigue**
  Assist cybersecurity personnel in assessing risk levels, focus on handling high-risk incidents.
- **Lighten Human Detection Burden**
  Automated intelligent threat hunting, proactively discover lurking threats in the environment.
- **Incident Mitigation, Minimize Losses**
  Prevent lateral movement, remediate threat damage.

## Features

### ① Continuous Monitoring, No Threats Can Hide

Through the engine's self-learning mechanism, it can automatically identify commonly used or new malicious programs and effectively detect encrypted files.

### ② Visualization to Quickly Identify Event Trajectories

By visualizing the path of attack, cybersecurity analysts can easily identify and gain a deeper understanding of the attacker's behavior, facilitating rapid incident recognition and enabling effective mitigation measures.

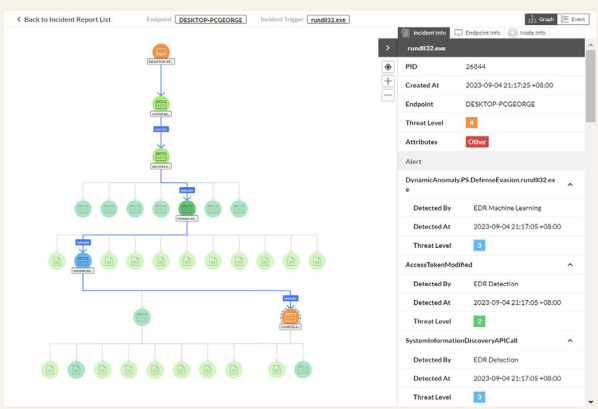
### ③ MITRE ATT&CK® Alignment for Accelerated Attack Investigation

Since each security event is tagged with the relevant ATT&CK tactics and techniques, the cybersecurity team can instantly assess the effectiveness of their defenses against certain adversary groups.

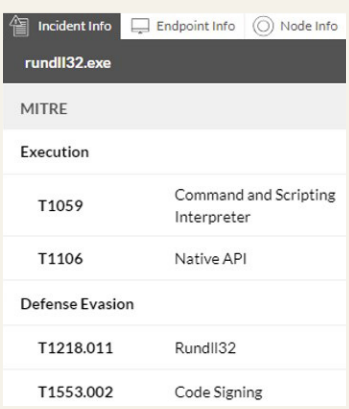
### ④ Timeline Presents the Overall Picture of Incidents

Through the event timeline, presenting in both node-focused and event-centric ways, the chronological analysis can speed up the incident investigation.

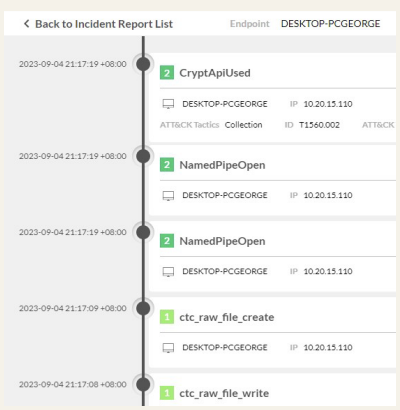
② Visualize network attack chains



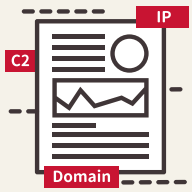

③ Align with MITRE ATT&CK®




④ Timeline view for incident investigation



## How does ThreatSonar comprehensively prevent ransomware attacks?

| Threat Prediction ▶ | Pre-compromise ▶ | Compromise ▶ | Post-compromise |
|---|---|---|---|
|  |  |  |  |
| **Threat Intelligence** | **Detect New Program** | **Real-time Response** | **System Restore Protection** |

### Continuously Predict Future Attacks, Precise Defense

By continuously monitoring the latest attack techniques of major adversary groups through the TeamT5 threat intelligence team, we stay ahead in predicting the next steps of ransomware attacks based on leading threat intelligence.

### Proactively Hunt Ransomware, Immediately Block Attacks

We can identify hundreds of ransomware programs and deploy trap files in the vicinity of protected files. If any unauthorized program attempts to access them, it will automatically trigger countermeasures, instantly terminating the processes and blocking malicious attempts to encrypt files.

### Halt Threat Propagation, Implement Immediate Isolation Measures

When a high-risk threat is detected, an instant alert is issued. If, through threat intelligence analysis, it's determined to be an attack, the malicious program is terminated, and the endpoint is isolated to prevent attackers from moving laterally within the network.

### Block Malicious Destruction, Effectively Safeguard Backup Data Restoration

With Windows VSS service, it rapidly enables backup mechanisms. When ThreatSonar Anti-Ransomware actively detects malicious attempts to damage backups, it promptly blocks such actions, ensuring the successful data restoration for businesses or organizations.

## 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