Datasheet

Incident Response

TEAMT5

Intelligence-Led, Comprehensive Incident Response

In order to expand the business and the collaboration with customers, enterprises and organizations have extensive use of network to provide services. However, hackers may exploit the network access to initiate attacks, causing operation shutdown and damaging brand value and customer rights. The incident response aims to reduce the losses caused by attacks and help the organization recover as soon as possible.

TeamT5 Incident Response Services - Professional Analysis, Investigation, Response

TeamT5, which has been researching global threat intelligence and tracking malware for a long time, has a deep understanding of organizations' incident response needs. Our professional Incident Response (IR) services help organizations quickly and effectively handle cyber incidents, protect critical digital assets, shorten the downtime of network services, and resume normal operations.

By deploying TeamT5's ThreatSonar Threat Forensic Analysis Platform, users can swiftly detect threats in the environment, starting the investigation from the compromised hosts to the overall security status of endpoints. Meanwhile, by analyzing key network logs, we clarify the possible access points of hackers and root causes, identify lateral movement, and evaluate the threat damage. We further provide suggestions on how to enhance security measures to defend against future similar attacks.

Preparation	Detection	Investigation and Response	Enhancement Suggestions
• Clarify incident status • Identify customers' requirement • Emergency containment suggestions • Provide IR plan	• Endpoint scan (ThreatSonar) • Collect and analyze critical evidences • Identify the compromise scope	• Sample analysis • Log analysis • Threat hunting • Identify root cause • Containment recommendations	• Expert-led incident analysis • Threat intelligence for defense • Root cause analysis and improvement suggestions

From Compliance to Prevention: The Strategic Importance of Incident Response

TeamT5's Incident Response services enable organizations to ensure compliance, secure critical evidence, conduct in-depth root cause analysis, and prevent future attacks with assurance.

Compliant with international security standards to drive efficiency

- IR process aligned with NIST SP 800-61r3, enhancing the efficiency of incident handling

Block threats and grasp the critical time to collect evidence

- Provide response suggestions immediately and collect critical evidence for incident retrospective
- Deploy ThreatSonar to quick scan threats in the environment

Comprehensively investigate suspicious threats to eliminate further attacks

- Begin with the investigation of main hacked hosts and identify the compromise scope
- Perform correlation investigation to check if there is any lateral movement

Professional and precise incident analysis to minimize damage

- Offer containment suggestions based on our research of adversary groups and TTP
- Recovery suggestions with proficient in handing in C2, stolen credentials and other types of attacks

Detailed incident investigation and prevention guidance

- IR experts conduct full incident reports, including root cause analysis and improvement suggestions
- Combine relevant intelligence and incident analysis to strengthen organizations' proactive defense

End-to-End Incident Response Services

From investigation to containment and analysis, addressing all aspects of incidents.

Offline, onsite, or remote investigations

- Preserve and analyze the logs and file system
- Identify the root cause and compromised hosts and provide the mitigation suggestions

System / Web / AP log analysis

- Find out the attack sources and patterns

Malware analysis

- Sandbox testing and expert manual analysis of provided samples.

TeamT5's IR Expertise Globally Recognized

Expertise in Incident Response	Over 20 years of malware and APT research, with hands-on incident response experience.
Industry-leading Adversary Research	We specialize in adversary analysis, threat hunting, vulnerability research, and root cause analysis.
Certified IR Professionals	Obtained multiple certificates, including OSCP, CCD, CCNA, CCNAS, CEH, CHFI, CTIA, ECSP, ISO 17025, etc.
Lecturer-level IR Expert	Speakers at international cybersecurity conferences including Black Hat (US), JSAC (Japan), CodeBlue (Japan).
World-class Industry Network	TeamT5 CSIRT is a member of FIRST, the world's largest incident response organization.

Experience in Handling Diverse Cyber Incidents

TeamT5 combines deep insight into threat trends with extensive experience in long-term investigations, covering incidents across industries and all-sized organizations.

APT Attacks	Website Hacking	Data Breaches	Compromised Devices
Ransomware	SQL Injection	VPN Credential Leaks	Phishing

ThreatSonar

ThreatSonar Threat Forensic Analysis Platform

Quick Scan, Efficient Incident Investigation

	Detected	Implemented	Over
	90%	**1 million+**	**1,000**
Benefits	Adopted by over **90%** managed security services providers in Taiwan	Implemented over **1 million** endpoints forensics	Successfully detected over **1,000** APT attacks missed by competitors

Industry-leading Features

Lightweight deployment and background execution without affecting daily operations

ThreatSonar agent can be deployed on thousands of computers and consumes minimal resources, allowing normal work during scans.

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, artifacts left on the host, and 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.

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.

Tel +886-2-7706-1299
E-mail sales@teamt5.org

TEAMT5 | THREAT INTELLIGENCE PIONEER, BORN IN ASIA