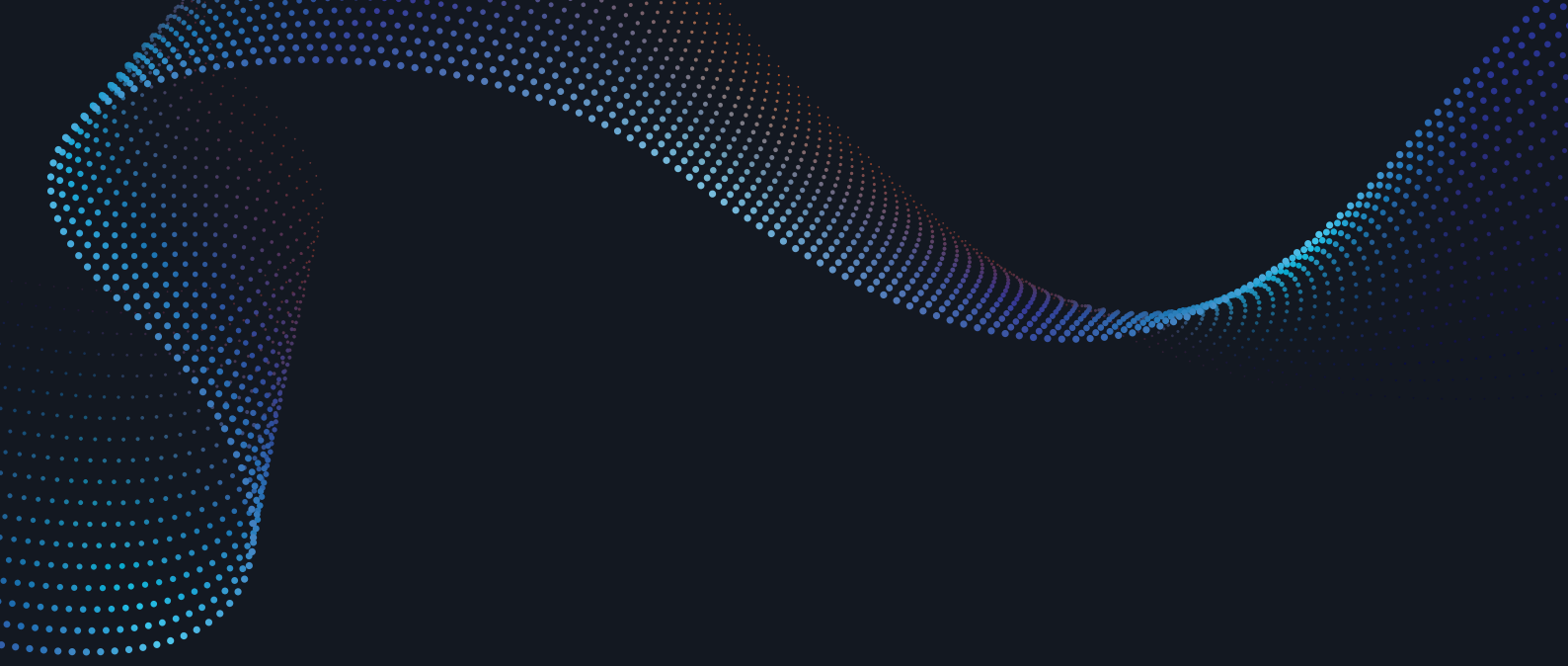


An abstract background graphic consisting of numerous thin, curved lines that sweep across the frame from the bottom left towards the top right. The lines are primarily blue, with a gradient that transitions into orange and yellow at the bottom right, creating a sense of motion and energy.

K7 THREAT INTEL FEED SERVICE

Contextual, Actionable, Threat Intelligence Feed that
Improves Threat Detection and Incident Investigation



THREAT INTELLIGENCE IS MUCH MORE THAN IOCs

An Indicator of Compromise (IOC) feed is noisy. It often consists of a deluge of seemingly disconnected information, overwhelming cybersecurity teams with a very large number of alerts, providing data without context, and resulting in alert fatigue. This increases the time and resources required for effective feed analysis and incident response thereby driving up cybersecurity risk and costs associated with breach damage control and business continuity.

Threat Intelligence enables a 30,000-foot view of enterprise threats, proactively gathering threat signals from multiple global sources, contextualising them, and abstracting information on malicious digital activity to pre-empt cyberattacks through actionable intelligence.

K7 THREAT INTEL FEED SERVICE



Predict



Detect

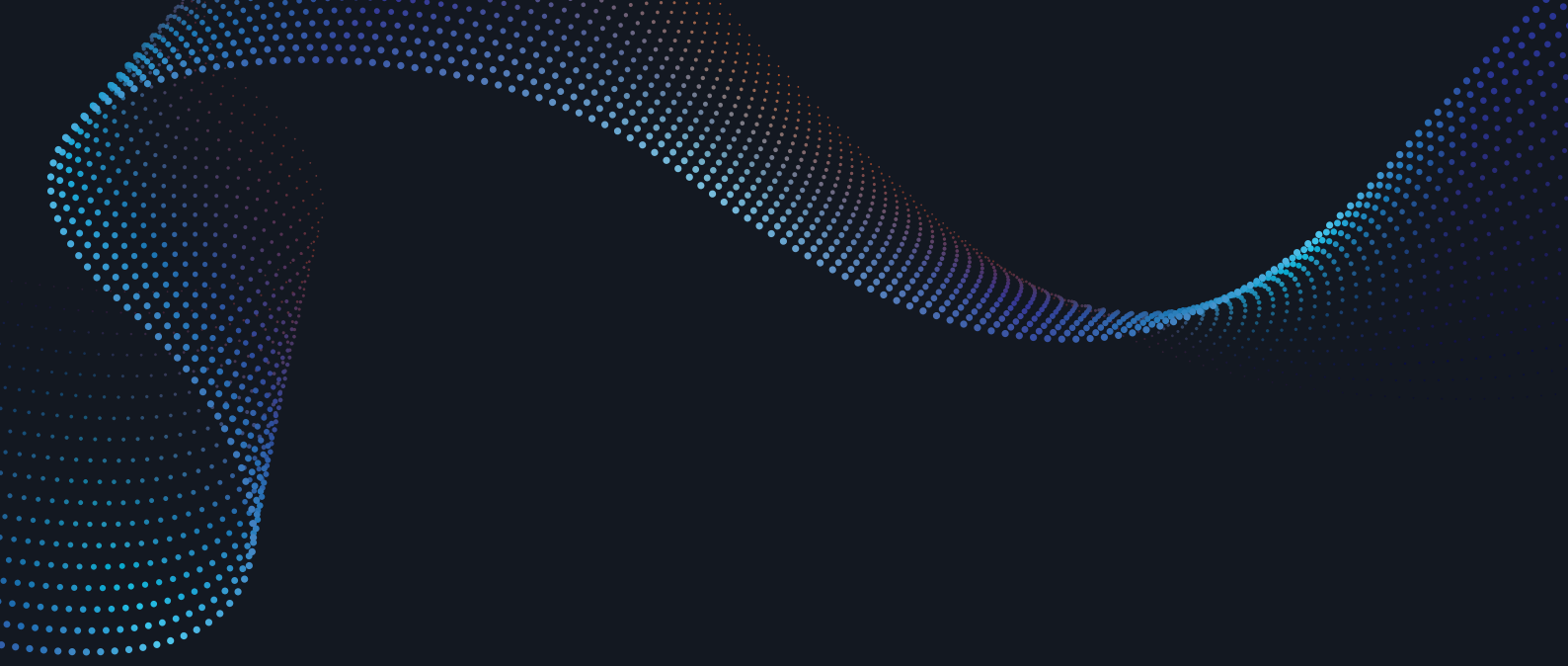


Prevent



Respond

K7 Threat Intel Feed Service (K7 TI) provides the big picture perspective that enterprise threat defence teams need to identify areas of concern before they turn into a cybersecurity incident, augmented by detailed threat information that enables rapid drill down to events or activities that require additional monitoring or specific response in the industry verticals and/or geographies of interest.



SERVICE OVERVIEW

K7 TI draws on K7 Security's over 30 years of experience in cybersecurity to provide relevant and appropriate information that helps cybersecurity teams identify, understand, and diagnose suspicious activity in the enterprise network.

Feed Types

Strategic Reports

High-level campaign overviews, and emerging trends

Tactical Indicators

IPs, domains, file hashes, CVEs, phishing URLs

Operational Alerts

Streaming via STIX/TAXII/JSON

Delivery Channels

STIX/TAXII/JSON feeds for automated ingestion

Data Sources

Telemetry data
from endpoints

Open and closed
darknet forums

Honeypots

Industry collaborations
and alliances

Delivery Frequency

Daily – Feed with
around 100,000
threat indicators

Weekly – Threat
Intelligence news

Monthly – Threat
Intelligence report,
by industry

Customers utilising K7
Endpoint Security also
receive Breach Intelligence
Protection alerts

TECHNICAL ARCHITECTURE & INTEGRATION

Data Ingestion	 Ingest data from distributed collectors across countries	 Aggregate raw feeds into a centralised data lake
Normalisation & Enrichment	 Parse IOCs into STIX objects	 Cross-reference with third-party datasets and darknet chatter
Delivery	 Push via STIX/TAXII/JSON with webhook support	

USE CASES



Threat Hunting

Leverage enriched TTPs to craft hypotheses and conduct proactive hunts



Incident Response

Automate IOC ingestion to accelerate containment and eradication



Vulnerability Management

Prioritise patching based on observed exploitation in the wild



Executive Reporting

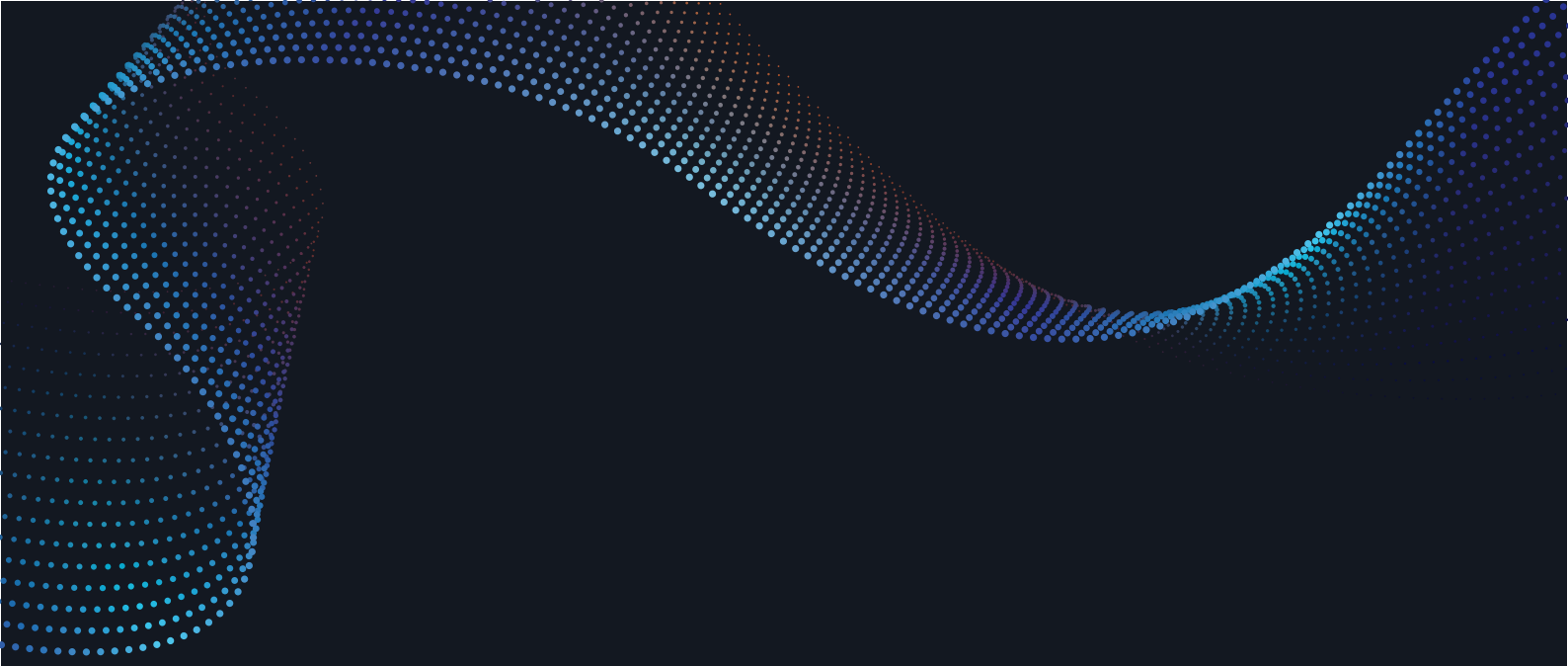
Summarise strategic threat intelligence for board-level decision making

DATA SOURCES



K7 TI's analysis is based on a broad spectrum of global and vetted data to deliver comprehensive intelligence that can function as an early warning system for emerging cyberthreats.

Threat signals are primarily obtained from K7's protection telemetry from millions of devices across the world; threat input sources include the Real-time Scanner, Behavioural Host Intrusion Protection System (HIPS), URL Block, Exploit Block, Firewall/Intrusion Detection System (IDS), Mobile Security Scanner, and the Spam Filter.



BENEFITS

Enterprise cybersecurity teams are often aware of an attack only after the attack begins, resulting in reactive crisis management rather than proactive threat prevention. K7 TI enables a bird's eye view to help cybersecurity practitioners identify and block a threat before it materialises. It also accelerates incident response in the event a threat actor does manage to launch an attack against the business, ensuring critical time immediately following an attack is spent repulsing the adversary instead of gathering attack information.

Proactive Cybersecurity
Management

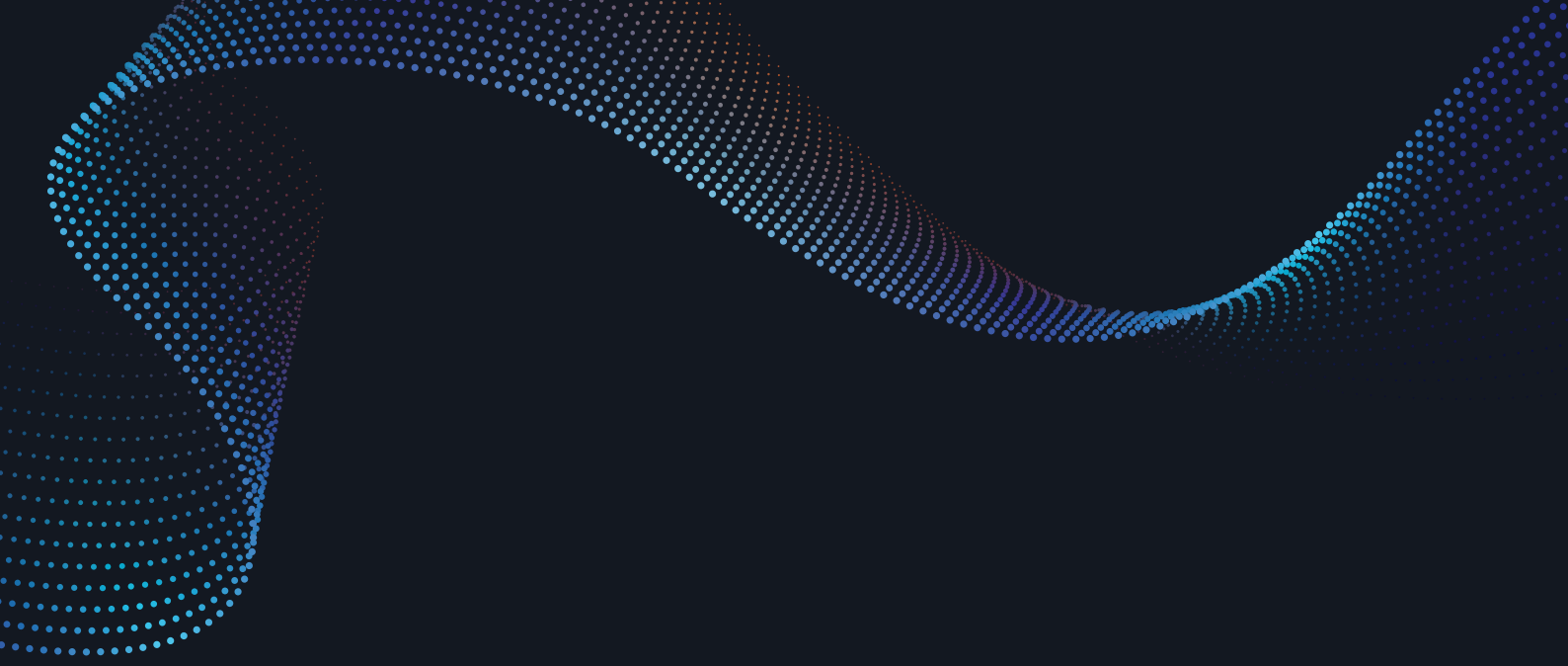
Access to Timely and
Specific Intelligence

Strengthens Security
Posture

Integrates into Existing
Security Operations
Centre (SOC)

Integrates into Existing
Security Information and Event
Management (SIEM) Solution

Can Be Fed into Network
Security Solutions



K7 TI IS THE SUPERIOR CHOICE FOR

Next Generation
Firewall Developers

SOC/SIEM Providers

Large Enterprise
Threat Monitoring Centres

ADVANTAGES

Enhanced **Security Event
Correlation**

Improved Threat Detection
with identification of
undetected malware

Early Attack Warning
through pattern identification

Rapid mapping of threats to
MITRE ATT&CK Framework

Reduction in Time and Effort
required for incident investigation

Reduction in False Positives
through contextual enrichment

Reduction in Noise
avoids alert fatigue

Enhanced **Playbook Automation**

Guides **Incident Response**
measures and prioritisation



WHY K7 IS THE PREFERRED ENTERPRISE CYBERSECURITY PARTNER

International Recognition

Awards



Associations & Partnerships



K7 Labs

Analyses hundreds of thousands of cyberthreat samples every day

Cutting-edge research backed by intelligent automated systems and machine learning

First discoverer of several malware. AMTSO RTTL Contributor Of The Year

World-renowned researchers

Knowledge sharing at Virus Bulletin, CARO, AMTSO, AVAR, and other international conferences

Patent-pending technology

Superior Trust

30+
Years

27
Countries

Global Telemetry
from Millions of Devices

World Class Cybersecurity – From India

100% Made In India

Only Indian Member –
Cyber Threat Alliance

Only Indian Programme Partner – Microsoft Azure
Sphere Security Research Challenge for IoT Vulnerabilities
and Microsoft Teams Vulnerability Challenge



The Global Cybersecurity Pioneer

India | Singapore | UAE | USA

www.k7computing.com