FOR IMMEDIATE RELEASE

November 5, 2026
KELA CO., LTD..

KELA Takes Pre-Attack Intelligence to the Next Level, Turning Early Attacker Signals into Action Before Cyberattacks Launch

Six new capabilities bring agentic AI to fusion-based threat hunting, investigation, built-in SOAR and early warning, turning attacker signals into decisive action and supporting Active Cyber Defense in Japan

---

TOKYO, November 5, 2026 — KELA Co., Ltd., the Japanese subsidiary of KELA Group, a global leader in cyber threat intelligence and exposure management, today announced six new capabilities that take pre-attack intelligence to the next level across the entire KELA CTI Platform. KELA also announced that KELA CONTROL, a first-of-its-kind fusion investigation and threat hunting platform, is now available to enterprises, together with a new managed intelligence service in which researchers from KELA's Cyber Intelligence Center (CIC) work closely with customers

The new capabilities help security teams see an attack while the attacker is still preparing it, investigate faster with agentic AI, and act automatically inside the platform. Together with KELA CONTROL, they follow KELA's approach to defense: anticipate attacks, act with precision and avoid the breach.

Background: early signs of attack in Japan

With Japan's Active Cyber Defense framework taking effect, organizations are expected to shift from responding after an incident to acting before one. At the same time, attackers are using AI to prepare attacks faster than ever. Every attack starts with people preparing it: scanning for targets, buying access and testing their tools. In Japan, KELA has recently observed this kind of preparation, including reconnaissance against internet-facing web and API assets and ransomware-related activity targeting VPN devices, as described in KELA's report Qilin and Japan: Attackers Probing Japanese Networks. These are early signals rather than confirmed compromises, and they give defenders a window to act, provided they can see the signals and decide quickly.

KELA CONTROL: fusion investigation and threat hunting, now available to enterprises

KELA CONTROL is a first-of-its-kind fusion investigation and threat hunting platform. It brings together three sources that are usually kept apart: KELA's data lake of more than 11 years of intelligence from the cybercrime underground, global network traffic data, and the customer's own sources. Agentic AI investigates across all three, mapping the connections automatically and following leads at machine speed, so analysts can run investigations that were not possible before: tracing the infrastructure attackers are building against their organization and turning weak signals into high-confidence findings.

With the new CIC managed service, KELA's CIC researchers run KELA CONTROL for customers who want the capability without building an in-house team: they investigate suspected attacker activity targeting the customer and deliver prioritized findings with recommended actions.

Six new capabilities in three directions

AI Augmentation: Faster, Deeper Investigation for Every Analyst
KELA AI puts an AI agent inside the platform to investigate, summarize and recommend next steps, and **Brand Control advanced analysis** uses AI to separate real impersonation and phishing from noise, with the reasoning behind every alert.

Pre-Emptive Early Warning: Seeing the Attack Before It Starts
Indicators Research returns a verdict with evidence on any IP, domain, URL or file hash in one query, and **Vulnerabilities Intelligence** shows which vulnerabilities attackers are actually exploiting, so teams patch what matters first.

AI-Powered Orchestration: Turning CTI into a Prevention Engine
MCP brings KELA intelligence into customers' own AI assistants, such as Claude, ChatGPT, Gemini and Copilot, and the **Integrations Portal** acts as a built-in SOAR, turning findings into automated response workflows inside KELA.

"Every attack begins with people who have a plan, long before the first alert," said Davidi Carmiel, Co-Founder & CEO of KELA. "KELA was built to see that preparation from the attacker's side. With six new capabilities across the platform, agentic AI and automation built into every step, and KELA CONTROL now available to enterprises with our CIC researchers running it for customers, organizations in Japan can anticipate attacks, act with precision and avoid the breach. Japan is one of KELA's most important markets, and we will keep investing in our customers and partners here."

About KELA

Founded in 2015, KELA provides intelligence-driven threat exposure management that makes malicious intent and activity transparent throughout the attack lifecycle. Using proprietary AI to process billions of data points on threat actors, infrastructure and techniques from the cybercrime underground, KELA gives organizations a true attacker's view to anticipate cyber attacks, take precise action and avoid the impact. KELA is part of KELA Group, together with ULTRARED (exposure management) and SLING (third-party risk management), and is trusted by government and enterprise security teams worldwide. KELA Co., Ltd., KELA's Japanese subsidiary, is based in Minato-ku, Tokyo. www.kelacyber.com

Media contact

KELA Co., Ltd. PR (Maeda / Nakamura)
Tel: +81-3-6634-7836

Email: jp-pr@ke-la.com