



Business Use Case

Insider Threats

In today's hybrid threat landscape, organizations in law enforcement, defense, forensics, and critical operations face sophisticated cognitive warfare. Adversaries deploy disinformation campaigns, hate speech, conspiracy theories, subtle psychological operations embedded in vast streams of open-source and sensitive textual data. These threats evolve slowly through weak signals, rising negativity, manipulations, emoji-coded intents, and semantic drifts, that traditional tools often miss until they escalate into real-world impacts like social division, targeted attacks, or eroded public trust.

Security teams struggle with data overload, dependency on foreign cloud platforms, hallucination-prone generative AI, and the risk of data exfiltration. Delayed detection means slower response times, compromised decision-making, and reduced operational resilience. A robust threat intelligence capability must enable early warning, deep inference, and autonomous action while maintaining full control over sensitive information. This is the core challenge Percipion addresses for European organizations committed to protecting sovereignty and societal cohesion.

To better detect insider threats, Percipion identifies grooming, coercion, psychological manipulation, and gradual disloyalty through deep analysis of internal communications. It detects rising negativity, emotional drift, and suspicious behavioral patterns, allowing security teams to intervene early and prevent data leaks, sabotage, or espionage from within.

Five Key Differentiators for Threat Intelligence

Percipion is a sovereign, symbolic cognitive platform developed by Aeteos after eight years of research. It faithfully reproduces human information processing mechanisms, drawing from neuroscience, psychology, linguistics, and philosophy, to transform sensitive textual data into actionable, human-like intelligence. Fully offline, explainable,

and EU AI Act compliant, it empowers operators with zero hallucinations and real-time foresight into emerging risks.

Sovereignty : Percipion delivers complete autonomy. Organizations can deploy their own instances without external dependencies or third-party components. This eliminates reliance on foreign providers, ensuring full data residency and control. In threat intelligence, this means national and organizational sovereignty over critical insights, enabling independent monitoring of cognitive and informational threats without risking strategic vulnerabilities.

Security : Designed for high-stakes environments, Percipion operates entirely offline with quantum-resistant encryption. It uses minimal power (only 2.37 Wh) and incorporates zero data capture. This poison-proof architecture prevents data leaks, external interference, or supply-chain attacks, providing unmatched protection for sensitive threat data in law enforcement, defense, and forensics operations.

Trustworthiness : Unlike probabilistic large language models, Percipion is knowledge-based and fully explainable. It uncovers weak semantics, psychological inferences, valences, hidden intents, and evolving patterns in text, transcribing allospeak and emojis accurately, while delivering transparent deterministic reasoning. Operators receive reliable, hallucination-free insights they can trust for high-consequence decisions, supporting human-led analysis or automated reasoned responses.

Sustainability: Percipion's efficient, low-energy design (2.37 Wh) makes it highly sustainable for continuous deployment in resource-constrained or field environments. By avoiding the massive computational demands of traditional AI, it reduces environmental impact while maintaining high performance, aligning with long-term operational and ecological resilience goals.

Legal: Fully aligned with the EU AI Act, Percipion prioritizes ethics, privacy, and compliance. Its transparent, human-centered approach ensures lawful use in threat intelligence workflows, minimizing regulatory risks and supporting ethical operations in forensics, law enforcement, and defense without compromising civil liberties.

Together, these differentiators strengthen resilience against cyber, cognitive, and informational threats, enabling faster detection, earlier warnings, and more informed decision-making.

Contact Aeteos today to explore how Percipion can enhance your threat intelligence capabilities and build a safer, more resilient Europe.