TARA INNOVA

Threat Intelligence Cloud

Threat Intelligence Without Blind Trust — Controlled, Validated, Enforced

The Challenge

Threat intelligence promises protection — subscribe to feeds, ingest indicators, block bad actors. Reality is messier. Thousands of indicators arrive daily, most stale or duplicated. External feeds provide no context. Sharing observations reveals your infrastructure. And intelligence sitting in a database isn't protection — the gap between "knowing" and "blocking" is where attacks succeed.

The Solution

TI Cloud coordinates threat intelligence across environments. It enables shared learning without blind trust in external feeds and without leaking local policy decisions. Intelligence that doesn't enforce is noise. TI Cloud closes the loop.

Key Capabilities

- **Controlled Synchronization** — Categorize feeds by origin and reliability, filter by indicator type, auto-expire stale data, resolve contradictions
- **Selective Adoption** — Auto-accept high-confidence indicators, queue medium-confidence for review, set score thresholds and geographic scope
- **Weighting & Validation** — Confidence scoring based on source reliability, cross-feed corroboration, recency, and your own enforcement results
- **Cross-Environment Learning** — Share intelligence across sites and tenants internally. Block in one, protect all
- **Privacy-Preserving Contribution** — Share indicators without exposing infrastructure — anonymized observations, aggregated statistics, opt-in per type
- **Direct Enforcement Integration** — Feeds directly into Quicksand and Oasis. No manual export. No enforcement gap

Enforcement Modes

Mode	Behavior
Block	High-confidence threats blocked immediately at the enforcement edge
Challenge	Medium-confidence indicators trigger PoW verification before access
Monitor	Low-confidence indicators logged and tracked for analysis
Enrich	Context added to traffic metadata without enforcement action

Intelligence Sources

- **Commercial Feeds** — Premium providers, industry-specific feeds, regional security organizations, vendor research
- **Open Source Intelligence** — Community blocklists, researcher publications, honeypot networks, abuse databases
- **Internal Observations** — Enforcement decisions, policy violations, failed authentication, anomaly detection alerts

- **Peer Networks** — ISACs, regional CERTs, partner organizations, managed security providers

Why TI Cloud

- **Control, Not Blind Trust** — Every indicator evaluated against your criteria before it affects your traffic.
- **Self-Improving** — False positives reduce scores, confirmed threats increase confidence. The system learns.
- **No Intelligence Leakage** — Contribute to collective defense without exposing your posture.
- **Zero Enforcement Gap** — Directly connected to enforcement points. Detection to blocking in seconds.

TARA INNOVA Kft. · www.tinnova.eu · sales@tinnova.eu · Book a Demo: tinnova.eu/sales