

 sada

 PiracyRemoval

AISA

 pureAi



 **reputeo**

An applied **AI lab** building its proprietary AI products for enterprise and institutional clients across security, intelligence, compliance, and digital asset protection.

Defense intelligence is fragmented across four stacks, none of them autonomous.

01 SOC drowning in alerts

10K+alerts/analyst/day·98% false positives

\$150K+/yr per analyst. 40% turnover.

Threat dwell time still measured in days.

02 External attack surface is invisible

Subdomains, certs, leaked creds, GitHub leaks

Discovery happens after exploitation.WHOIS / SSL / DNS
ingestion is manual and stale.

03 Reputation & web monitoring is manual

Reports written by hand. Days to insight.

Comms, brand, M&A, and security teams still query
separately. No real-time, no chat layer.

04 IP & content piracy goes unprotected

Weeks to take down. Lost revenue compounds.

Detection is partial; takedowns are manual; legal
evidence is collected after the fact.

Every CISO buys 4+ vendors. None of them talk to eachother.

Defense intelligence is fragmented across four stacks, none of them autonomous.

01 SOC drowning in alerts

10K+alerts/analyst/day·98% false positives

\$150K+/yr per analyst. 40% turnover.

Threat dwell time still measured in days.

02 External attack surface is invisible

Subdomains, certs, leaked creds, GitHub leaks

Discovery happens after exploitation.WHOIS / SSL / DNS
ingestion is manual and stale.

03 Reputation & web monitoring is manual

Reports written by hand. Days to insight.

Comms, brand, M&A, and security teams still query
separately. No real-time, no chat layer.

04 IP & content piracy goes unprotected

Weeks to take down. Lost revenue compounds.

Detection is partial; takedowns are manual; legal
evidence is collected after the fact.

Every CISO buys 4+ vendors. None of them talk to eachother.

What we are

An AI lab building practical, high-impact AI products for real-world challenges.

It designs the data pipelines, detection logic, and application layer around the AI, engineers the products end to end, and integrates them into each customer's environment - taking responsibility for how its systems behave in production.

End-to-end engineering

Engineering is carried out internally - systems are designed, built, validated, and operated by Reputeo's own team.

Applied research

Across AI, cybersecurity, software engineering, data science, and digital investigations - running pipelines and models in production.

Solutions for real problems

Not deployed on benchmarks alone - models are evaluated against representative, real-world data before production.



Strategy

Four products, one engine,
and why that’s a 10× advantage.

1.	2.	3.	4.
Engineering leverage	Customer compounding	Defensibility via switching cost	Speed to new verticals
One AI/OSINT core powers all four modules. Every model improvement, every new data source, every reasoning capability ships across the platform. Unit economics improve with each release.	A telecom buys AISA, then expands into PureAI, then Piracy Removal - same account team, same data flywheel, same console. Net dollar retention compounds; CAC amortizes across modules.	One evidence vault. One integration set. One unified analyst console. The more modules a customer activates, the more painful it becomes to leave - a structural moat.	New use case = new product on the same engine, not a new company. We have shipped four production modules in 36 months. The fifth is faster than the first.

This is why Reputeo is one company - not four. The platform is the product.





IVAN KADIĆ
CEO & Co-Founder



Founded in
Belgrade in 2022.
Engineering-first.
Built for the B2B world.

thereputeo.com

Applied AI. Built to run in production.

Reputeo runs on proprietary AI products - already built, already in production. For each client, we configure and adapt them to fit specific workflows, data and constraints.

Deployed on your infrastructure or as an external layer - you keep full control, while AI cuts manual work and sharpens decisions.

Team overview

Led by PhDs in physics and computer science, our multidisciplinary team brings together engineers and specialists from top technical product, growth and research institutions, with backgrounds in software engineering, electrical and computer engineering, telecommunications, and international relations.



Neda Trifunović
COO

Marija Mitrović Dankulov
AI Lead

Anđelko Simić
CTO





An AI Lab of 30+ engineers focused on one thing: building AI systems that actually work inside real organizations.

ISO 9001 · 27001 · 27701 · 42001

thereputeo.com

Where we focus



Data & Document intelligence

On-prem AI platform for forensic search and compliance work across internal documents - with optional reach into the open web to monitor reputation and brand signals when required.



Cybersecurity

Two AI products that augment SOC analysts, accelerate detection across multi-source telemetry, and continuously score domain and IP risk — turning raw threat data into operational intelligence.



Digital Piracy

AI that monitors marketplaces, social platforms and the open web for unauthorized distribution of digital content - classifies infringement at scale and feeds takedown workflows for legal and brand teams.

AISA



What it does

Continuous OSINT scanning of domains, subdomains, certificates, IP/ASN blocks, leaked credentials, GitHub leaks, and brand-abuse patterns. Real-time risk scoring with graph-based correlation linking distant events into a single incident view.

Why it wins

Cuts threat-discovery from weeks to minutes. Verified OSINT- based evidence, ready for legal takedowns. Compliance- aligned with NIS2, DORA, and the EU AI Act.

Who needs it

CISOs, compliance teams, brand protection, M&A diligence, legal departments - anyone responsible for an external attack surface or regulated digital footprint.

Validation and output

Multiple production deployments across 3+ regions. Live security telemetry in critical infrastructure. CyberE71 cybersecurity finalist at GITEX Global Dubai 2025.

Most enterprise customers enter Reputeo OS through AISA - then expand into adjacent modules.

AISA

Virtual SOC analyst.



CYBERSECURITY

What it does

Continuously monitors security telemetry, interprets signals with context, correlates events, assesses risk, recommends precise actions, and learns from every outcome. A senior analyst working every second of every day.

Why it wins

Full incident reasoning, classification, and reporting - not just detection. Works with existing security stacks. Continuous learning advantage compounds. Sovereign-deployment ready.

Who needs it

Critical infrastructure: telecom, finance, energy, government, large enterprise. Sectors with continuous-uptime mandates and regulator-driven SOC requirements.

Validation and output

Production-deployed with enterprise customers. Output includes interactive dashboards, compliance alerts, and takedown-ready evidence packages.

Expansion product. Lands cleanly with existing AISA customers and stand-alone with compliance buyers.



What it does

Upload contracts, reports, or internal data - or point it at the open web. SADA classifies, extracts, scores risk, and answers any question in plain language. Forensic audit on MSAs, SOWs, amendments. Live web monitoring with mobile alerts.

Why it wins

Cross-document reasoning detects governance gaps - missing audit clauses, partial enforcement language, risky amendments. Source-linked answers in real time. Weeks of analyst work compressed into minutes of conversation.

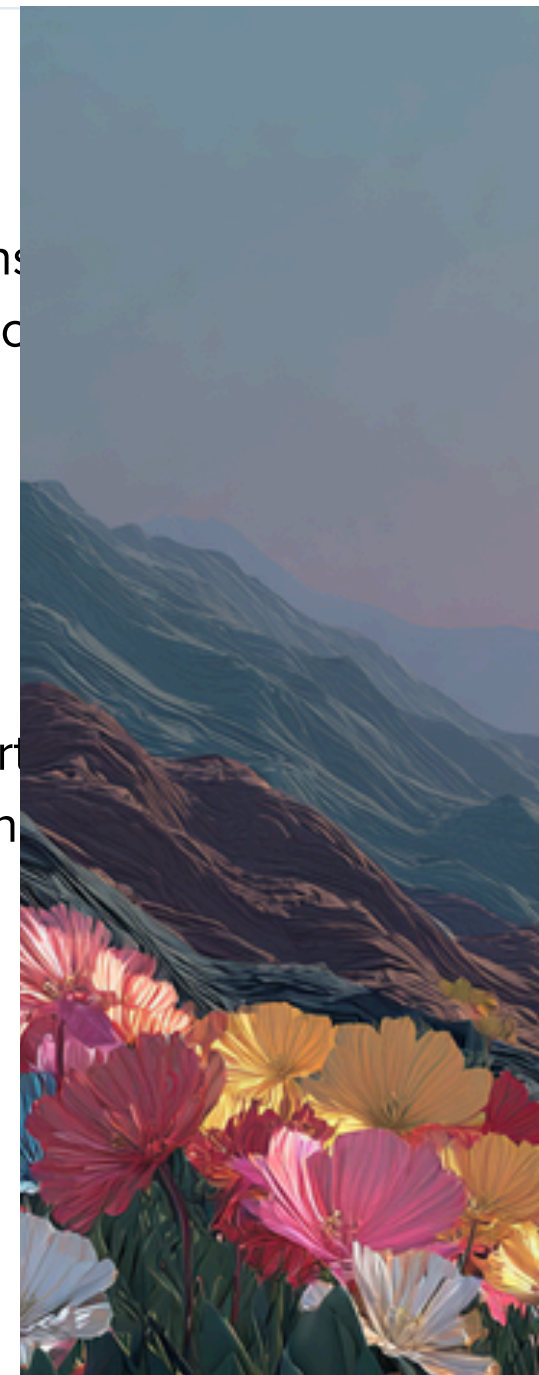
Who needs it

Legal, compliance, audit, procurement, communications, executive protection, security - anyone interrogating documents or the web faster than analysts can.

Validation and output

Live forensic-audit deployments analyzing contract portfolios for enterprise clients. Web monitoring tracking thousands of topics, brands, and individuals concurrently.

Cross-vertical product. Same engine sells into Legal & Audit and Comms & Security - proof the platform generalizes.





What it does

AI-driven detection of unauthorized digital distribution across sport streams, IPTV, multimedia, web and social media platforms. Automated takedown procedures with legal-evidence collection in a single loop.

Why it wins

End-to-end: detection, automated takedown, and audit-grade evidence - not just monitoring. Real-time dashboard with content removed and ROI on revenue protected.

Who needs it

Rights holders, broadcasters, sports leagues, premium-content studios, and software vendors. Sectors where unprotected revenue is measured in tens of millions per quarter.

Validation and output

Live deployments with enterprise rights holders. Output measured in volume of removed content and reduction in unauthorized stream availability.

Traction

\$700K → \$1.5M ARR in one year. ~\$3M raised. 28 in Belgrade.

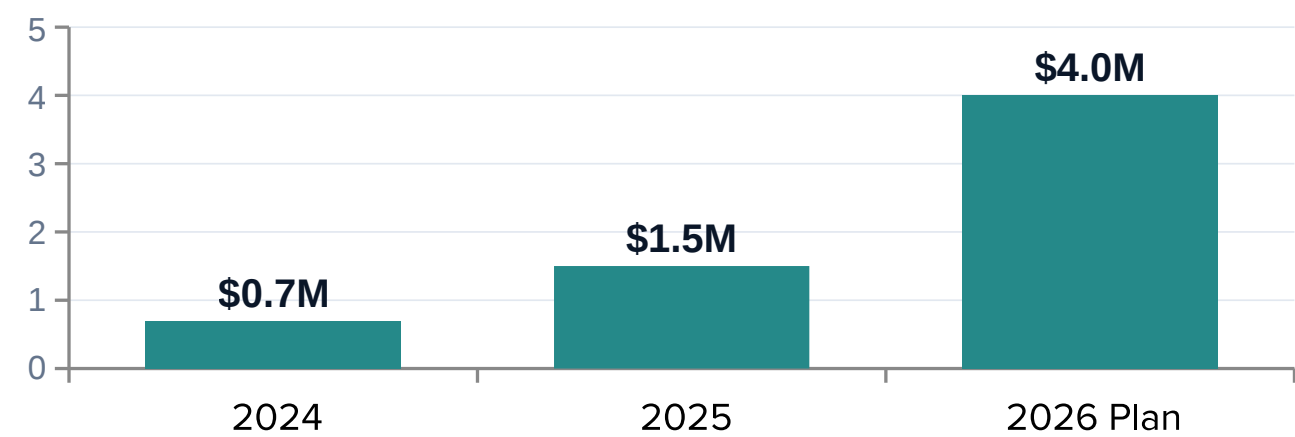
\$1.5M

+114%

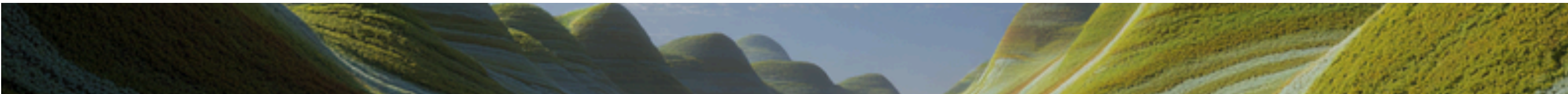
~\$3M
PROOF POINTS

28
PEOPLE

ARR TRAJECTORY



- Revenue balanced across all four product modules - platform thesis already monetizing.
- Production deployments across 3+ regions, including critical infrastructure.
- Customers across telecom, finance, government, and rights-holder sectors.
- CyberE71 finalist · GITEX Global Dubai 2025 · ISO 27001 / 27701 / 9001 / 42001.



Sitting at the
intersection of three
structural growth
markets.

~\$15B

~12% CAGR

EXTERNAL THREAT INTEL & BRAND PROTECTION

Brand abuse, OSINT driven exposure, attack-surface management. PureAI + SADA serve this segment.

DIGITAL PIRACY & IP PROTECTION

Rights-holder demand for autonomous takedown. Piracy Removal serves this segment.

~\$2B+

Accelerating with
streaming & sports
rights inflation

\$50B+

AI security budgets
growing +45% YoY

CYBERSECURITY - SOC

CISO consolidation pressure.
Replacement cycle for legacy
SIEM. AISA serves this segment.

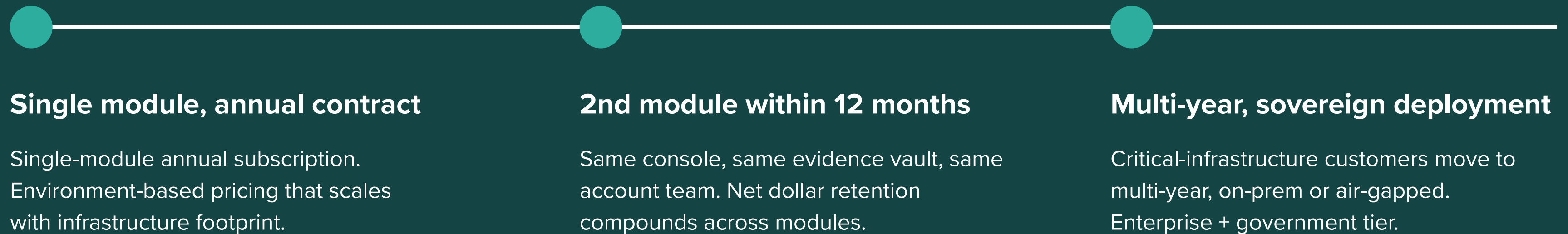
Total cybersecurity spend tops \$200B globally. The structural trend is platform consolidation - CISOs are vendor-fatigued and replacing point tools with control layers.

Business model

SaaS subscriptions.

Multi-module expansion.

Sovereign-deployment optionality.



CHANNELS

- **Direct enterprise sales** - telecom, finance, energy, large corporates
- **Government & defense** - national cyber agencies, critical infrastructure operators
- **Strategic partners** - MSSPs, system integrators, cloud providers

GEOGRAPHIC PRIORITIES

- **EU - NIS2 / DORA** tailwind, sovereign-deployment demand
- **Middle East** - critical-infra capex, sovereign cloud
- **US - scale layer**; CIRCIA + sector compliance

Thank You

Cybersecurity and intelligence are
converging - at machine speed.
We're building the operating system that
runs underneath.



Please reach out at

ivan@thereputeo.com

www.thereputeo.com