



ChaosAI

AI-Powered Autonomous Penetration Testing

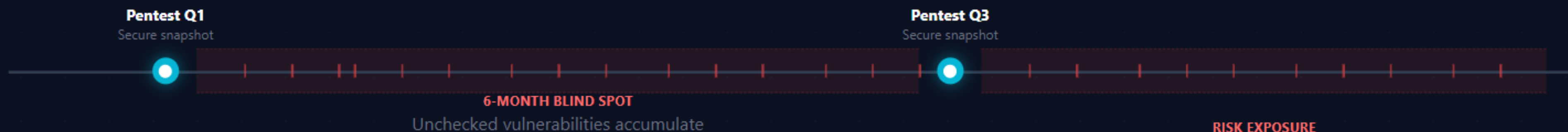
FEBRUARY 2026

Security Testing Is Stuck in 2010

The attack surface evolves faster than humans can test it.

TYPICAL ORGANIZATION TIMELINE (1 YEAR)

Manual Pentest Infra Change / Deployment



Infrequent Snapshots

Traditional pentests happen only 1-2x/year. New vulnerabilities go unnoticed for months between tests.



Alert Fatigue

Automated scanners generate thousands of low-context findings, drowning engineers in noise.



Scaling Bottleneck

Hiring skilled security engineers is expensive and slow. Teams can't scale linearly with cloud growth.

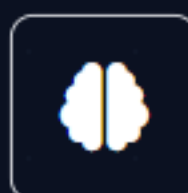
The Innovation Gap

Bridging the divide between human expertise and machine speed.

LEGACY OPTION A

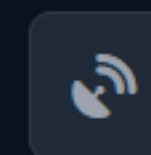
APPROACH
Manual Pentest

- ✓ **High Accuracy**
Human intuition finds complex logic bugs
- ✗ **Infrequent (1-2x/Yr)**
Leaves massive time gaps for attackers
- ✗ **Expensive & Unscalable**
€15k+ per test, linear headcount scaling

OUR SOLUTION
Autonomous AI

- ∞ **Continuous Testing**
24/7 coverage like a scanner
- 🎯 **Human-Like Accuracy**
AI agents validate findings (low noise)
- 🚀 **Scalable & Contextual**
Adapts to infra changes instantly

LEGACY OPTION B

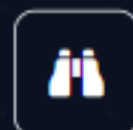
APPROACH
Auto Scanners

- ✓ **High Frequency**
Runs daily or on every commit
- ✗ **High Noise (False Positives)**
Requires manual triage of thousands of alerts
- ✗ **Low Context**
Doesn't understand business logic

PROBLEM: Organizations are forced to choose between **quality** and **speed**.

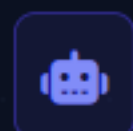
AI-Native Autonomous Pentesting Platform

Continuous intelligence. Human-grade accuracy.



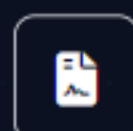
Continuous Reconnaissance

Automatically maps your entire attack surface: domains, subdomains, and APIs, in real-time as you deploy.



Intelligent Testing Agents

Multi-step autonomous agents that think like attackers, chaining exploits to validate true risk without the noise.



Actionable Insights

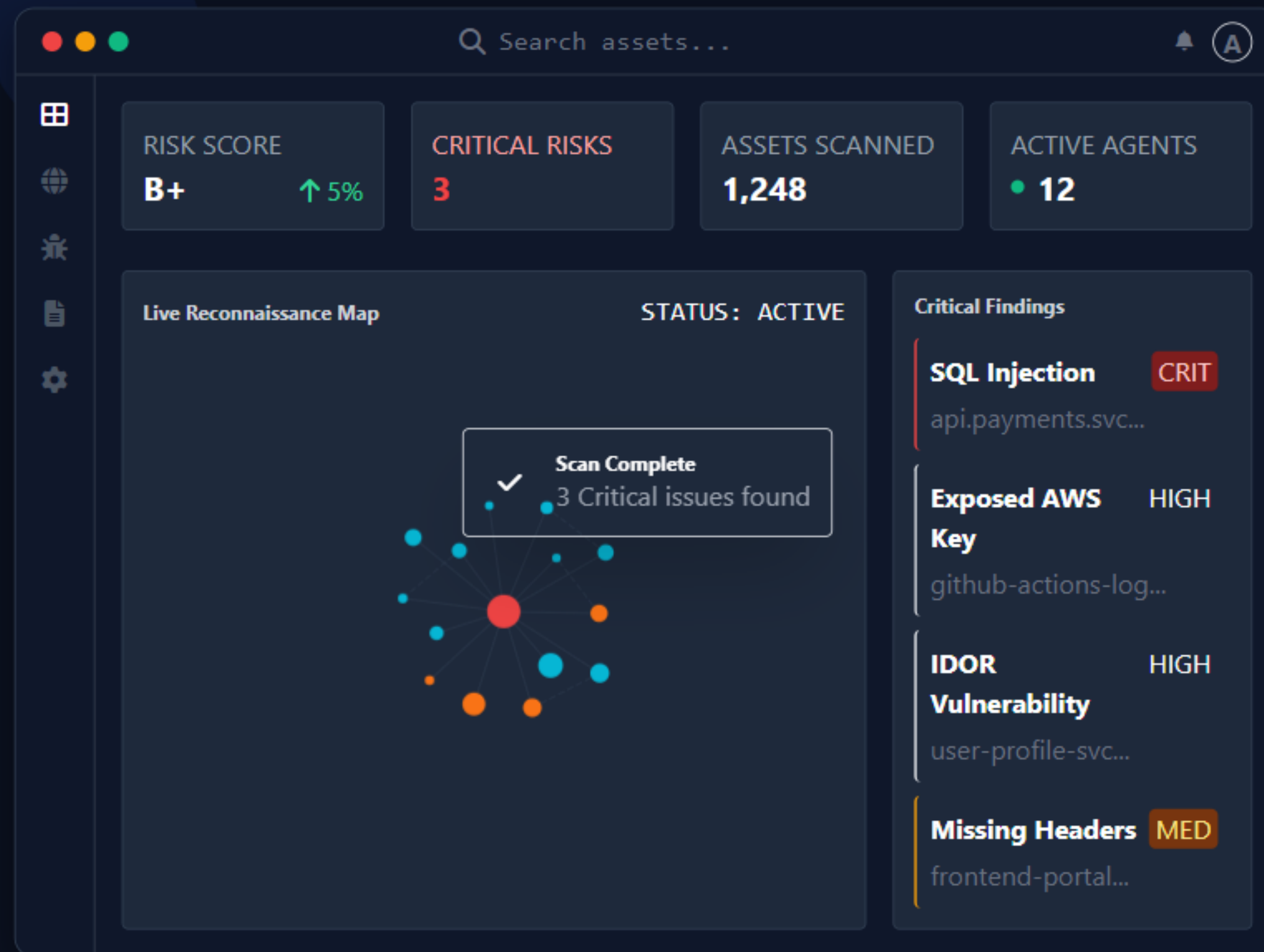
Prioritized, human-readable reports with remediation code snippets. Integrated directly into Jira and Slack.

10x

TEAM OUTPUT

Daily

TESTING CYCLES



How It Works

From blind spots to prioritized insights in three autonomous steps.



RECONNAISSANCE

Discover & Monitor

Autonomous agents continuously scan domains, subdomains, cloud buckets, and APIs to map your evolving attack surface in real-time.



INTELLIGENCE

Analyze & Validate

AI logic engines attempt benign exploitation chains to validate risks, filtering out 99% of false positives found by traditional scanners.



REMEDIATION

Prioritize & Act

Deliver executive summaries and developer-ready fix code. Integration pushes validated tickets directly to Jira, Slack, or SIEM.

● Raw Asset Data

● AI Verification Loop

● Verified Vulnerabilities

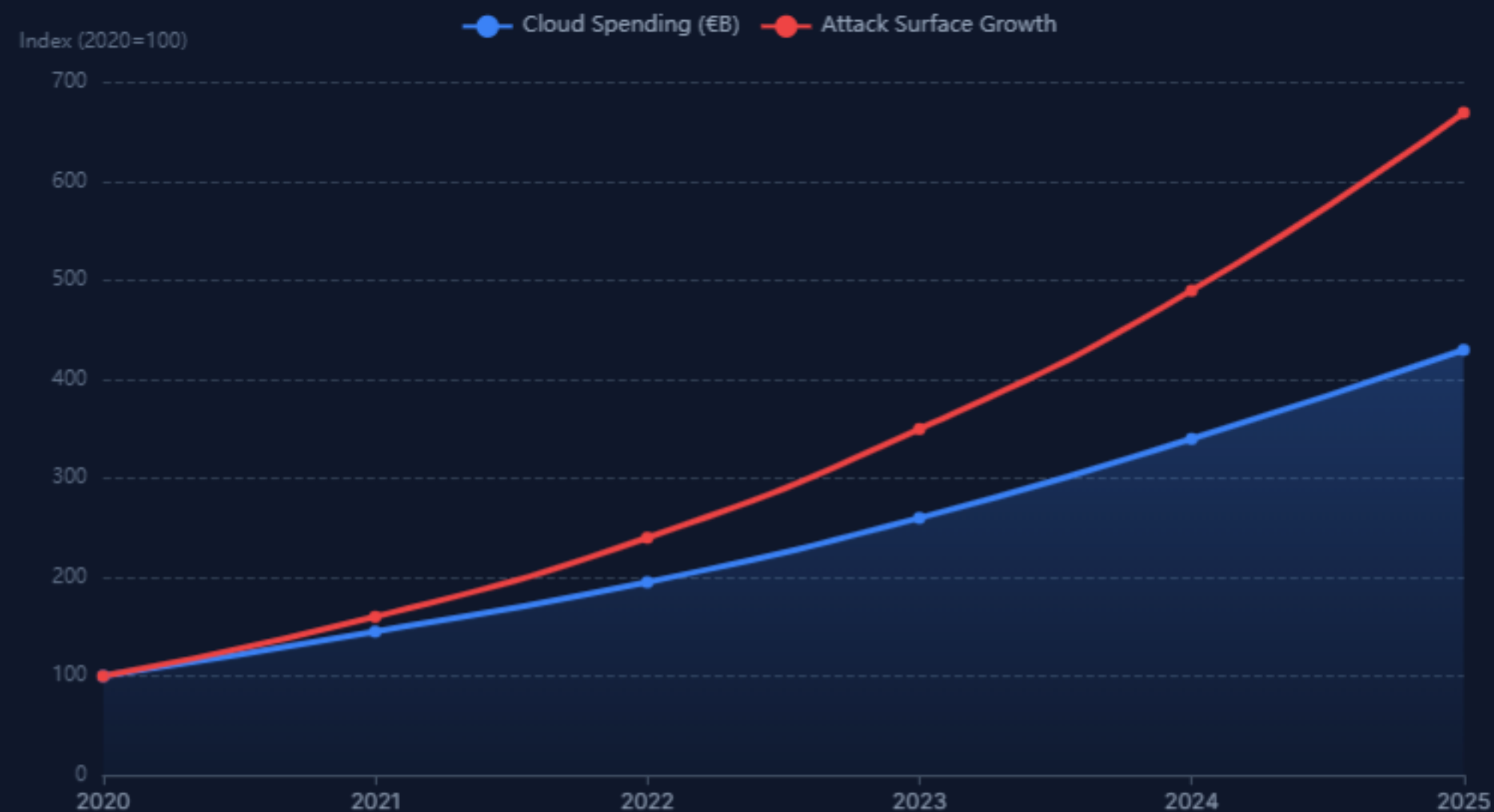
Why Now?



INFRASTRUCTURE SHIFT

Cloud Spending vs Attack Surface

Global cloud spending reached €600B+ in 2023, but attack surfaces are growing 50% faster than security budgets can handle.



A perfect storm of technological shift and market necessity.



Talent Crisis

Unfilled Cybersecurity Jobs (US)

500K+

↑ Growing YoY

"There simply aren't enough humans to secure the code we write."



Compliance

SOC 2, ISO 27001, and PCI-DSS 4.0 now demand **continuous** monitoring, not just annual checks.

SOC2

ISO

PCI



AI Maturity

LLMs enable agents to understand business logic, bridging the gap between **dumb scanners** and humans.

Tech Readiness

The Billion-Dollar Gap

Capturing the white space between manual services and automated tools.

TAM
€200B+
Global Cybersecurity

SAM
€3B+
Pentesting Market

SOM
€500M+
Cloud-First Mid-Market

MACRO TREND

Cybersecurity spend is resilient to downturns.

OUR WEDGE

Cloud-First Mid-Market with complex infrastructure but limited budgets.

MARKET GROWTH

15.2% CAGR
2024-2030

KEY DRIVERS

Scanner fatigue • SOC 2 compliance • Cloud complexity

Scalable SaaS Revenue

Tiered subscription model aligned with scan volume and enterprise needs.

Free

€0 / month

Individual developers & small teams

✓ 10 scans per month

✓ Basic reporting (PDF)

✓ Community support

✓ Single user

Target: Developers

MOST POPULAR

Premium

€10-€50 / user / mo

Growing teams & startups

✓ Unlimited scans

✓ AI remediation code

✓ Priority support

✓ Jira & CI/CD integration

✓ API access

Target: Startups & SMBs

Enterprise

€10-50K / year

5 free users included · Annual license

✓ Custom compliance mapping

✓ Custom deployment (VPC / on-prem)

✓ Dedicated support & TAM

✓ SSO & audit logs

Target: Enterprise

PRIMARY CUSTOMER SEGMENTS

- Cloud-First Startups
- Mid-Sized Tech
- MSSPs (Channel)
- + Fintech / Healthtech

PRICING DRIVERS (UPSELL LEVERS)

- Scan Volume
- Frequency
- Analysis Depth
- Integrations

Commercial Traction & Strategic Pipeline

From validation to revenue: a clear path forward.

✓

Autonomous Engine v1.0
End-to-end recon & AI-driven reporting, zero human intervention

✓

100+ Full-Cycle Operations
Validated reliability & false-positive reduction in controlled environments

🚀

Live Pilots

HIGH INTENT

Active, live-environment pilot projects with technical professionals validating the platform.

TCS

Global IT services leader testing autonomous pentesting in production environments.

Active Pilot

Mediolanum

Irish financial services firm validating continuous security testing.

Active Pilot

🏢

Enterprise Pipeline

WARM LEADS

Exploratory discussions with high-value licensing targets across critical infrastructure.

Irish Water

National water utility, critical infrastructure security.

Former Employer

Core Idea Origin

★

Crane Logistics

Supply chain security validation

Lyca Mobile

Telecom infrastructure testing

McMonagle Stone

Manufacturing sector security

🔧

Technical Partners

ECOSYSTEM

Non-commercial technical partnerships validating infrastructure and architecture.

TCS

Technical validation of autonomous pentesting capabilities.

Technical Validation

📄

AWS

Cloud infrastructure partnership for scalable deployment.

Technical Validation

🍷

Apple

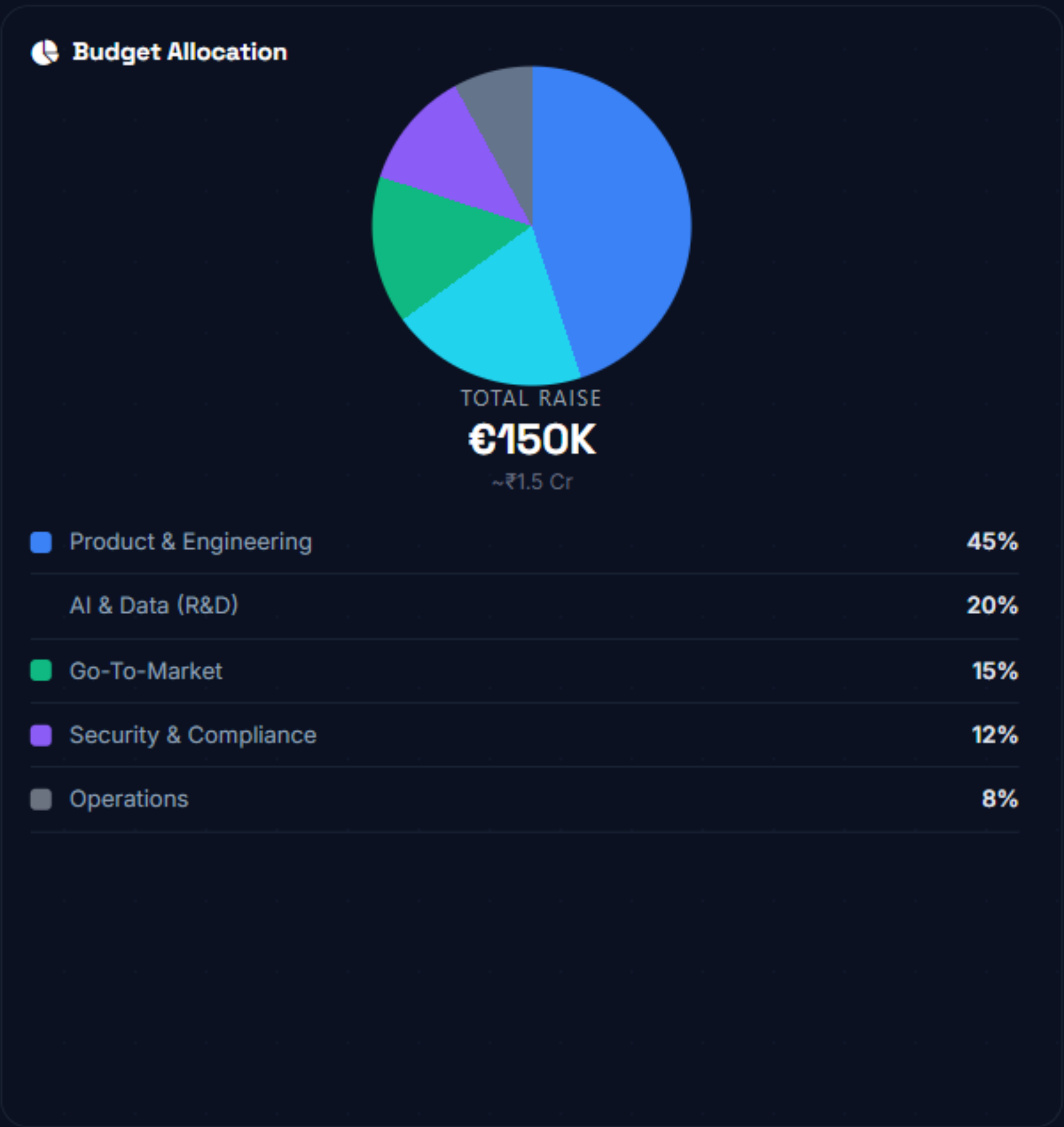
Platform integration and security architecture consultation.

Technical Validation

🍏

€150K Seed Round

Capital allocation to reach product-market fit and first revenue in 12 months.



12-Month Execution Roadmap

ON TRACK

MONTH 3

Pilot Conversion
Harden platform for production. Convert TCS & Mediolanum pilots into paying Premium users.

Production Ready

MONTH 6

First Enterprise Deal
Close first enterprise license. Complete SOC 2 readiness. Expand agent capabilities (API testing).

€25K ARR

MONTH 12

Scale & Next Round
15-30 Premium users + 2-4 enterprise deals. Proven GTM motion. Ready for Series A.

€50K+ ARR

PMF VALIDATED

Go-To-Market Execution Plan

How we get there: two parallel motions to first revenue.



Zero-CAC Conversions

€2K-€10K

REVENUE TARGET

15-30 Premium users @ €10-€50/mo

HOW: PRODUCTION DEPLOYMENT 8-12 Wks

Security Hardening

Scale Testing

Monitoring & SLAs

Backup & DR

Domain-Specific AI Agents



Enterprise Licensing

€20K-€100K

REVENUE TARGET

2-4 deals @ €10K-€50K/year

HOW: ENTERPRISE SANITIZATION 6-10 Wks

SOC 2 / ISO / GDPR

MSAs & SLAs

Audit Trail

Custom Deploy

Harden beta into production → pilots convert to paying users automatically.

Compliance & legal readiness → unlock enterprise contracts.

PILOT CONV.

100%

ENT. DEALS

2-4

ARR TARGET

€50K+

TO REVENUE

14-22w

Technical Founder, Full-Stack Vision

**Shubham Rao****Founder & CEO**

EY · AWS · Irish Gov

AWS SA · MS SOC · Sec+

Cloud and AI engineer with experience building and securing large-scale infrastructure on AWS for enterprise clients. Previously held senior cloud engineering roles at EY and Irish Government, scaling systems for millions of users.

The idea for ChaosAI came from working at Irish Water, where critical infrastructure teams relied on infrequent, expensive pentests while their attack surface evolved daily.

CORE EXPERTISE

Cloud Infra

LLMs & AI Agents

SecOps

Python

Building the tool I needed when I was on the other side.

Why I Can Execute

The right background at the right time.

**Founder-Market Fit**

I've been the engineer scrambling after a pentest report drops. At Irish Water, I saw the gap between what security teams need and what they actually get. ChaosAI addresses that directly.

**AI-Native, Not AI-Wrapped**

Deep technical background in both LLM agent architecture and cloud security. Built the autonomous engine from recon to reporting, and it's already running live pilots with enterprise clients.

**Proven Execution Velocity**

From concept to working prototype to live pilots at TCS and Mediolanum. Shipping daily based on real feedback from production environments.

VALIDATED BY

TCS

AWS

Apple

Mediolanum

The Future of ChaosAI: A Unified Security Platform

From autonomous pentesting to complete security automation.

ChaosAI's autonomous pentesting tool is the **foundational layer** for a massive platform, automating offense, compliance, and defense in one AI-native system.

**Offense**

CURRENT

Automating the attacker's perspective for the most accurate risk data.

Autonomous Pentesting

Red Teaming Agents


Continuous Recon

Exploit Chains

Zero-Day Detection

STATUS

• Live

**GRC**

NEXT

Translate raw technical data into audit-ready evidence for SOC 2 & ISO.

GRC Agents

Cloud GRC


Auto Compliance

SOC 2 / ISO Evidence

Risk Quantification

TIMELINE

Q3-Q4 2026

**Defense**

LONG-TERM

Offensive data trains defensive agents to autonomously patch vulnerabilities.

Blue Teaming Agents

LLM Defense

Auto-Remediation

Patch Generation

Continuous Hardening

TIMELINE

2027+

**The Billion-Dollar Vision**

One platform. Three pillars. Complete security automation.

MARKET OPPORTUNITY

Join Our Journey

WE ARE RAISING

€150K



~₹1.5 Cr

Seed Round

OUR VISION

"To make continuous, autonomous security testing the industry standard, bridging the gap between manual expertise and automated scale."

LET'S BUILD TOGETHER

 director@entropyresearch.ai www.chaosai.dev

Building the future of autonomous security testing.

The Plan (12 Months)

Product

Ship production platform & expand agent capabilities

Customers

Convert pilots + close 2-4 enterprise deals

Revenue

Reach €50K+ ARR with dual GTM motion

Milestone

Validate PMF & prepare for Series A

★ Why Invest Now



Founder-Market Fit

Deep experience in Cloud, AI, and Security from EY, AWS, and Irish Government.



Live Pilots & Pipeline

TCS & Mediolanum actively validating. Enterprise pipeline with Irish Water, Crane, Lyca.



Market Tailwinds

Exploding cloud adoption + talent shortage + compliance pressure = perfect timing.



Massive Upside

Targeting the multi-billion dollar gap between scanners and consultancies.