# Cyber start-up Innerworks raises $4m to fight AI-powered fraud with “synthetic” defences



London-based cybersecurity start-up Innerworks has raised $4m in fresh seed funding to expand a novel approach it calls Synthetic Threat Intelligence. The round was led by AlbionVC, with participation from Digital Currency Group, Founders Capital, Firestreak Ventures, NVTBL Ventures, Metaversal Ventures and senior executives from Citi, UBS, Coinbase, Checkout.com, Apple and Crypto.com. Reports put the raise at about €3.4m–€3.7m depending on conversion.

The company argues that generative AI has supercharged online deception, enabling bots and fraudsters to mimic legitimate behaviour. “We’re facing AI-powered deception that can mimic legitimate users with frightening accuracy,” said Oliver Quie, Innerworks co-founder and chief executive. “Existing security companies have become obsolete because they assume threats will behave differently from legitimate users.”

Innerworks’ platform combines device fingerprinting, bot detection, VPN and proof-of-personhood signals with geolocation analytics. A continuous RedTeam programme feeds adversarial bypasses back into detection libraries so the models learn from the tactics of their opponents. The company claims a 97% detection rate against advanced AI threats, though these figures have yet to be independently verified.

Unlike standard bug-bounty programmes, RedTeam operates as a decentralised, gamified subnet on the Bittensor network. Contributors submit adversarial solutions, which are tested in sandbox environments; successful entries are added to open-source defensive libraries and rewarded with TAO tokens. The firm says the model accelerates learning and strengthens defences in real time.

Early traction has come through partnerships in payments and digital assets. Innerworks lists Crypto.com as a client, and incident-response specialist ZeroShadow described a strategic alliance with the firm after the ByBit incident to improve stolen-funds tracing and freezing.

Investor enthusiasm is strong. “We invested in Innerworks because they’re not incrementally improving fraud detection, they’re fundamentally reimagining it,” said Cat McDonald, partner at AlbionVC.

The company plans to use the funding to grow its RedTeam ecosystem, develop products and scale into major financial centres, highlighting ease of deployment through a minimal-code npm package.

Questions remain over regulatory acceptance of token-based incentives, procurement standards for financial institutions and the need for independent benchmarking of performance claims. Yet if Innerworks can deliver on its promises, it could position the UK at the forefront of responsible AI security — blending adversarial research with practical protection for banks, exchanges and online platforms.

Created by [Amplify](https://www.hbmadvisory.com/amplify): AI-augmented, human-curated content.

## Bibliography

1. <https://siliconcanals.com/uks-innerworks-lands-3-4m/> - Please view link - unable to able to access data
2. <https://siliconcanals.com/uks-innerworks-lands-3-4m/> - Silicon Canals reports that Innerworks, a London cybersecurity startup pioneering Synthetic Threat Intelligence, raised €3.4m in a seed round to protect financial services from fraud, bots and sanctioned actors. The piece notes AlbionVC led the financing with participation from other investors, and quotes AlbionVC on Innerworks’ novel approach. It summarises the firm’s RedTeam ethical‑hacking ecosystem and product suite — bot detection, device fingerprinting and geolocation intelligence — claiming high accuracy against AI‑driven threats. Founders Oliver Quie, Oscar Hayek and Tom Ryan are named, and the company’s plans to scale product development and global partnerships are outlined over the next year.
3. <https://www.eu-startups.com/2025/08/london-based-cybersecurity-startup-innerworks-raise-e3-7-million-aiming-to-stop-ai-fraud-in-its-tracks/> - EU‑Startups covers Innerworks’ €3.7m seed round led by AlbionVC and lists participation from Digital Currency Group, Founders Capital, Firestreak Ventures, NVTBL Ventures and Metaversal Ventures, plus senior executives from major banks and tech firms. The article describes Innerworks’ Synthetic Threat Intelligence and its RedTeam decentralised bounty platform for adversarial training. It cites claims that the company’s bot detection, device fingerprinting and geolocation capabilities outperform market leaders and reports a reported c.97% detection rate against advanced AI threats. Founders Oliver Quie, Oscar Hayek and Tom Ryan are profiled and the piece outlines planned product expansion and strategic partnerships with financial institutions.
4. <https://www.globenewswire.com/news-release/2024/12/23/3001462/0/en/Innerworks-and-Bittensor-Join-Forces-to-Launch-RedTeam-A-Decentralized-Hub-for-Cybersecurity-Innovation.html> - GlobeNewswire published Innerworks’ press release announcing a partnership with Bittensor to launch RedTeam, a decentralised platform that gamifies cybersecurity by rewarding ethical hackers with TAO tokens for bypassing detection systems. The announcement explains how RedTeam incentivises researchers to submit code that uncovers vulnerabilities, which are then integrated into open‑source libraries to strengthen detection models. It highlights Innerworks’ focus on next‑generation bot detection and behavioural analytics and frames the subnet as a means to accelerate adversarial training and real‑world defence against AI‑enabled threats. The release includes quotes from Innerworks’ founders emphasising rapid innovation and collaborative security development across the finance sector.
5. <https://www.innerworks.me/> - Innerworks’ official website explains its mission to eliminate bad actors using Synthetic Threat Intelligence, offering device fingerprinting, VPN detection, bot detection and proof of personhood. The site emphasises seamless integration via an npm package and minimal code changes so the service runs unobtrusively behind apps and websites. It highlights RedTeam as an ethical hacking programme used to continuously battle‑test detection models and states the platform provides high‑precision risk signals from thousands of real‑time data points. The homepage lists partnerships and ‘trusted by’ logos from crypto and payments firms and invites prospective customers to book demos to deploy its defensive technology.
6. <https://www.zeroshadow.io/post/innerworks-announces-partnership-with-zeroshadow> - ZeroShadow’s blog post describes a strategic alliance with Innerworks following the Bybit exploit, explaining how the partnership combines ZeroShadow’s incident response and attribution capabilities with Innerworks’ device fingerprinting and behavioural detection. The post outlines plans to use combined intelligence to identify and freeze stolen funds, assist exchanges in tracing malicious actors and strengthen defences across the crypto ecosystem. It quotes Innerworks’ CEO Oliver Quie on leveraging high‑precision fingerprinting and highlights ZeroShadow’s experience investigating major hacks, listing its client base and emphasising the collaboration’s potential to disrupt DPRK‑linked laundering operations and improve proactive protection for victims and platforms globally over time.
7. <https://docs.theredteam.io/> - RedTeam’s documentation explains the technical architecture and operation of the Innerworks‑run subnet on Bittensor, detailing miner and validator roles, submission processes and challenge templates for decentralised adversarial testing. It describes how miners submit encrypted solutions, validators evaluate submissions in sandboxed environments and how scoring, emissions and point decay incentivise continuous improvement. The docs provide setup guides for running nodes, integration examples and challenge templates that mirror real‑world bypass scenarios to harden detection models. The repository stresses open‑source contribution, reproducible evaluation and seamless incorporation of successful exploits into production models to accelerate defensive capability against evolving AI threats in production environments.