Escape raises $18M Series A from Balderton to fight AI-powered cyberattacks with AI agents

- Escape's offensive security engineering platform replaces legacy systems with continuous, AI agent-driven discovery, pentesting and remediation
- As cyber threats continue to rise globally, the funding will help Escape accelerate software development to aid overstretched security teams

New York, 10 March, 2026: Escape, the offensive security engineering platform, has raised $18 million in Series A funding to automate the entire security lifecycle with AI agents. The round, led by Balderton with participation from Uncorrelated Ventures and existing investors IRIS and Y Combinator, will help lean security teams fight back at a time when code is being written and attacked at an ever-increasing pace; according to Check Point Research, organisations are now facing an average of 1,968 cyber attacks per week, an increase of 70% since 2023.

AI has compressed the window between code being shipped and vulnerabilities being exploited to hours. While recent industry shifts have focused on securing code at the developer's IDE, it's only part of the story. Attackers exploit live systems targeting real configurations, integrations, authentication flows and business logic that only exist in production. Escape's AI agents operate exactly here: mimicking the behaviour of a sophisticated attacker to find exploitable logic flaws and data leaks that exist only in live environments, and remediating before attackers get to them first.

Point-in-time pentesting and fragmented legacy tools can't keep pace, leaving security teams who are currently outnumbered 100-to-1 by developers, overwhelmed and exposed. CEO Tristan Kalos and CTO Antoine Carossio – both Forbes 30 under 30 alumni and with extensive machine learning and security expertise between them – founded Escape to fix this broken model by replacing legacy scanners and manual offensive security processes with AI agents that automate the full lifecycle. Tristan has experience as a machine learning engineer and data scientist working in Spain and France, while Antoine has extensive cybersecurity experience from working with the French government and the Computer Research Institute of Montreal (CRIM).

Fighting fire with fire

Escape's agents continuously discover, test and fix vulnerabilities directly within engineering workflows. They automate attack surface discovery, continuous security testing, and contextual remediation. Instead of generating a report that sits in a queue, Escape's agents keep the system moving from the moment a vulnerability is found to the moment it's fixed. In this way, Escape multiplies the impact of security teams at scale, without increasing headcount or alerts.

To put the scale of the threat into perspective, Escape's team recently uncovered more than 2,000 high-impact vulnerabilities hidden in 5,600 publicly available vibe-coded applications. This included 175 instances where personal data was exposed, often with several sensitive secrets revealed at once. Every vulnerability was present in live production systems and discoverable in hours.

Suranga Chandratillake, partner at Balderton Capital, said: “The days of pen-testing being a sporadic, manually driven process are over. As the number of software developers (both human and agentic) explodes, security teams find themselves with an impossible dilemma: rely on legacy scanners, knowing they do not have the quality of pen-testing or continue to work with manual offensive security teams and fail to scale to the volume of code being written. Escape has solved this challenge with the world's first AI-native, offensive security platform that blends the scalability and relentless capacity of technology with the ingenuity of your security team. We are hugely impressed with how rapidly Escape has become a trusted platform for sophisticated organisations around the world and look forward to partnering with the team to further their work.”

Trusted globally

Escape is trusted by 2,000+ security teams globally, including BetterHelp, PandaDoc, CyberCube, Arkose Labs and more. One recent customer and global leader in its field saw a 393% ROI after deploying Escape, shrinking its security testing processes from five days to five hours. While edtech platform Thinkific is using Escape to secure its applications end-to-end and gain visibility into vulnerabilities while embedding continuous, developer-friendly security testing into its workflow.

In total, Escape now runs more than 300,000 security assessments a month across its global base, which can equate to days of manual testing that security teams get back every month.

Tristan Kalos, CEO and co-founder of Escape, said: "Security teams are outnumbered and drowning in siloed, manual processes. In a world where code is written and attacked at the speed of AI, this cannot continue. We are building Escape as the offensive security engineering platform to solve that problem at scale.”

Daniel Ilies, IT Security Engineer at Visma, said*:* "Escape's IDOR scanning and multi-tenant capabilities set it apart from other security testing solutions. We can test multiple scenarios that simply aren't possible elsewhere. We've fully automated team onboarding with project-scoped permissions, and the team is incredibly responsive to feedback and actually implements it."

The Series A will deepen the platform's AI agent capabilities, including agentic pentesting that reasons about application logic rather than scanning for known patterns, and scaling the engineering and go-to-market teams to meet growing enterprise demand in the US and Europe.

Contact: sayula@burlington.cc

About Escape

Escape is pioneering offensive security engineering, a new approach that replaces legacy scanners and manual processes with AI agents that discover, test, and remediate vulnerabilities directly in engineering workflows. Built for security teams that are 100x outnumbered by developers, Escape automates the full offensive security lifecycle so teams can multiply their impact without scaling headcount. Learn more at escape.tech.

About Balderton

Balderton Capital is a multistage venture firm with more than 25 years of experience supporting Europe's best founders from Seed to IPO. We have both early and growth funds and invest across the technology sector, with a proven track record backing AI, fintech, B2B SaaS, digital health, mobility, gaming and marketplace companies. Previous investments include Darktrace (LON: DARK), Depop, Dream Games, Flywire (NASDAQ: FLYW), GoCardless, Kobalt, MySQL, Nutmeg, Peakon, Recorded Future, Talend (NASDAQ: TLND) and THG (LON: THG). Balderton's current portfolio includes: Exein, Fuse Energy, Proxima Fusion, Quantum Systems, Revolut, Stream, Taktile, Wayve and The Exploration Company. https://www.balderton.com/

About Uncorrelated Ventures

Uncorrelated Ventures is an early-stage venture capital firm focused on backing technical founders building data-driven and infrastructure-first companies. The firm partners with entrepreneurs at the earliest stages, supporting them as they build category-defining businesses across enterprise software, AI and security. Uncorrelated takes a high-conviction, concentrated approach and works closely with founders from day one to help them scale. https://uncorrelated.com/