Solution Overview

APOLLO

AI-Powered Continuous Automated Red Teaming Platform

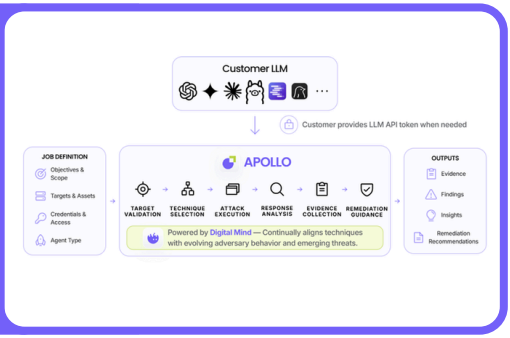
Discover Unknown Attack Paths Before Real Adversaries Do

Every breach begins with a compromise. Every compromise follows a path. Discover the path. Eliminate the risk.

APOLLO is an AI-powered Continuous Automated Red Teaming (CART) platform that continuously emulates how real adversaries could compromise your environment. Rather than relying on periodic red team engagements, APOLLO safely executes realistic adversary techniques across production environments to identify exploitable weaknesses and produce evidence where defenses fail. Powered by Digital Mind, every assessment reflects the latest adversary tactics, ensuring testing remains aligned with today's evolving threat landscape.

APOLLO safely executes repeatable adversary techniques across production environments using purpose-built offensive security automation, delivering scalable, production-safe testing without consuming customer LLM tokens.

For complex attack scenarios, APOLLO leverages customer-provided frontier AI models to make contextual decisions during attack execution, extending testing beyond traditional automation.



By combining offensive security automation with frontier AI reasoning, APOLLO delivers continuous adversary emulation that scales efficiently while applying AI where contextual reasoning delivers the greatest value.

With APOLLO, organizations understand how real adversaries could compromise their environment before attackers do. Security teams receive evidence-backed guidance to prioritize remediation, while leadership gains measurable confidence in the organization's cyber resilience.

AI CAPABILITIES IN APOLLO

- **TARA AI:** The Autonomous CTEM Agent behind APOLLO. Security teams define objectives through natural language while TARA AI orchestrates adversary emulation, automatically creating the appropriate jobs based on customer objectives and approved guardrails.
- **Frontier AI Reasoning:** Leverages customer-provided frontier AI models to make contextual decisions during complex attack scenarios, enabling realistic testing of dynamic applications, authentication workflows, and evolving target responses.
- **Digital Mind:** Continuously aligns attack techniques with current adversary intelligence, ensuring every assessment reflects evolving attacker tactics without manual updates or threat feed management.

Product Highlights

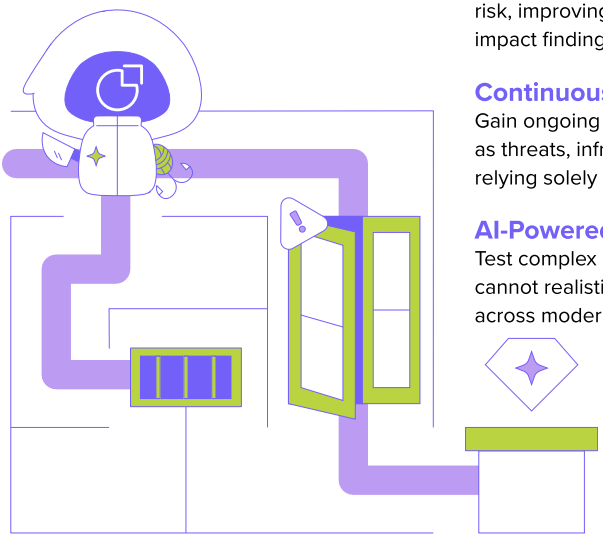
Continuous Adversary Emulation
Continuously emulates realistic adversary techniques across production environments, including exploitation, authenticated application attacks, API attacks, and post-exploitation activities, producing evidence of successful compromise across diverse attack scenarios.

Comprehensive Threat Coverage
Powered by Digital Mind, APOLLO continuously aligns attack techniques with evolving adversary behavior, ensuring every assessment reflects today's threat landscape and remains relevant against emerging attacker techniques and tactics.

Automated Attack Simulation
Safely executes repeatable adversary techniques across production environments, adapting to target responses where required while producing objective evidence of successful compromise without disrupting normal business operations or critical services.

Evidence & Remediation Guidance
Every assessment produces evidence of successful compromise together with prioritized remediation guidance, delivering actionable findings that help security teams quickly eliminate critical weaknesses and strengthen organizational resilience.

Platform Advantages



Exploitability Validation
Focus remediation on the vulnerabilities that pose the greatest risk, improving efficiency and reducing time spent on low-impact findings.

Continuous Security Assurance
Gain ongoing confidence that critical systems remain resilient as threats, infrastructure, and applications evolve, without relying solely on periodic security assessments.

AI-Powered Offensive Testing
Test complex attack scenarios that traditional automation cannot realistically emulate, expanding security coverage across modern applications and APIs

Evidence Driven Remediation
Transform successful exploit evidence into prioritized remediation guidance, helping security teams resolve the exposures with the greatest impact on organizational risk.

> *We moved from annual exercises to daily assurance.* **APOLLO** *surfaces the real risks and lets our team remediate what matters most.*
>
> —— **Head of Security Operations**

www.digidations.com
info@digidations.com

digiDations is an AI Native cybersecurity company helping organizations move from hoping their defenses will hold to knowing they will through Autonomous Cyber Defense.