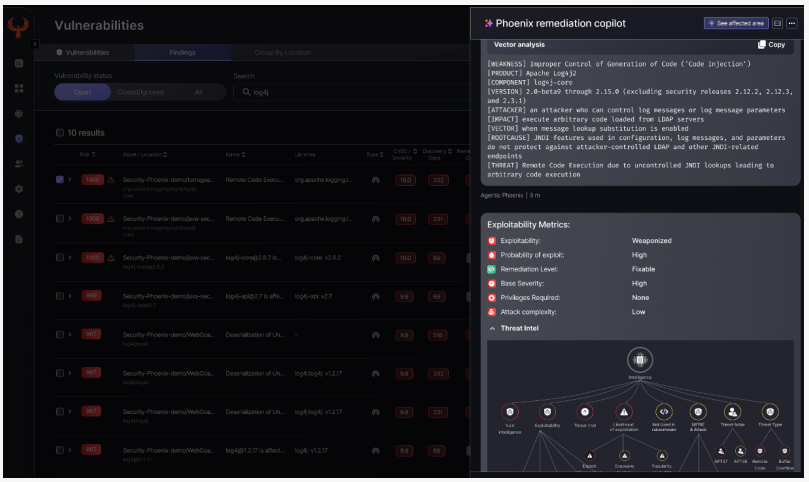
Phoenix Security’s AI Agents to Automatically identify Vulnerabiluty Patterns that leads to exploitation and ransomware

From mapping vulnerabilities to threat actors with 10x remediation speed, Phoenix’s AI Agents slash noise by up to 98% while keeping analysts in control.



AI Agent Analyzer Phoenix Security

LONDON, UNITED KINGDOM, September 22, 2025 / EINPresswire.com/ -- Phoenix Security, the leader in Application Security Posture Management (ASPM), is raising the bar for AI in security operations with the launch of its intelligent, human-aligned AI Agents. Designed to work alongside security teams—not sideline them—these agents have already driven dramatic results, delivering up to 98% noise reduction, 96–99% fewer criticals, and 430,000+ engineering hours reclaimed for customers like ClearBank, Bazaarvoice, and others in the Retail and Banking sectors.

> “Anyone can point an LLM at a CVE feed. We built 3 AI agents that think like seasoned analysts—connecting vulnerabilities, ingesting context, delivering fixes developers can use immediately,”
>
> *Francesco Cipollone CEO & Co Founder Phoenix Security*

This isn’t about dumping AI on top of vulnerability data. It’s about precision, context and acceleration—turning raw findings into targeted and actionable steps that fit directly into the way teams already operate.

Three Agents. One Mission: Multiply Analyst Impact
Phoenix’s AI-powered trio—The Researcher, The Analyzer, and The Remediator—work in concert to take security teams from detection to resolution with speed and surgical accuracy.

- The Researcher (available now) continuously monitors real-time threat intelligence, both public and private, mapping attack methodologies, including MITRE&ATTACK, correlating vulnerabilities to active attack methods, ransomware campaigns, known threat actors

and other relevant attack methodologies. Proprietary models developed in partnership with Google deliver exploitation prediction on ransomware and likelihood of exploitation compensating EPSS metrics. It goes beyond CVE summaries, tracing root causes and filtering the noise, so teams can focus on true business-critical risks. The researcher agent has been trained on top of Google's vast intelligence, adding prediction elements related to ransomware and active exploitation. The agent has the widest mapping to CWE, MITRE and threat actors, allowing it to predict the ransomware likelihood before a vulnerability gets exploited

Phoenix ASPM AI Agents Cybersecurity

Phenix Security Case Studies

- The Analyzer models attack paths and threat modelling within the actual business and application context, empowered by Phoenix Security's code-to-cloud contextual AI engine. The analyzer reveals which vulnerabilities are impacting in the particular application context, delivering STRIED threat modelling and attack scenarios that are rooted in real data, real-time context, and not just 'in theory'.

- The Remediator transforms that context into environment-specific remediation plans, leveraging the researcher and the analyzer, to produce an executable bundle of remediation by similar remedy, attack path, and logical assets. The remediation also works alongside you, producing compensating controls that are considered based on the deployment context. Remediaitor also outputs in Jira, Service Now, and a remediation campaign to empower the security team to be on top of the remediation efforts.

Proven Results Across Industries
ClearBank cut container noise by 98%, eliminated up to 99% of criticals and saved $2.6M in analyst time annually—equivalent to four hours per security engineer, every week.

Bazaarvoice eradicated all critical vulnerabilities in two weeks and reduced high-risk findings by 40%, creating immediate alignment between security and engineering.

Ad-Tech giant achieved a 78% reduction in container vulnerabilities while unifying code and

cloud visibility.

The Phoenix Difference: Threat-Centric, Context-Driven, Human-Aligned
While others push generic AI assistants, Phoenix Security's agents enrich vulnerabilities with threat actor mapping, ransomware risk prediction, and contextual remediation intelligence. The approach blends automation with analyst oversight, ensuring decisions are grounded in operational reality.

This agentic architecture, already proven to accelerate remediation 10x faster, allows CISOs and AppSec leaders to keep control while scaling their team's capability. Instead of chasing thousands of alerts, teams get a surgical set of prioritized actions per team—fully enriched with ownership, risk context, and actionable fixes.

Phoenix Security's AI Agents are already available to customers, with the Researcher live today and the Analyzer and Remediator rolling out in 2025. The result: faster remediation, measurable risk reduction, and teams spending more time solving problems than sifting through noise.

Phil Moroni
Phoenix Security
+1 919-594-8888
email us here