Prophet Security Automates Detection Engineering with AI Detection Engineer, Expanding Its Agentic AI SOC Platform

AI agents continuously find detection gaps, build and validate detections, tune rules, and create live MITRE ATT&CK coverage map from completed investigations

Prophet Security Logo

LAS VEGAS AND PALO ALTO, CA, UNITED STATES, July 30, 2026 /EINPresswire.com/ -- AI Detection Engineer in Brief:

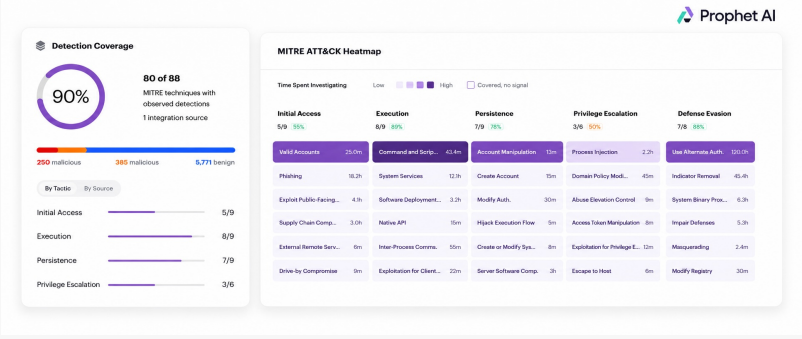
- Automates the detection engineering lifecycle by identifying coverage gaps, authoring new detections, tuning existing rules, and validating every recommendation based on organizational policy.
- Keeps security teams in control by allowing organizations to choose the level of AI autonomy while maintaining review, version control, backtesting, and rollback capabilities.
- Builds a continuous MITRE ATT&CK coverage map using completed investigations and threat hunting results to reveal the difference between coverage organizations have and coverage they only appear to have.

> AI Detection Engineer turns detection engineering from an occasional project into a continuous operational capability."
>
> *Grant Oviatt, Co-Founder and Vice President of Product, Prophet Security*

Black Hat 2026 USA - Prophet Security, the pioneer in Agentic AI for Security Operations, today announced the general availability of AI Detection Engineer, a new product within the Prophet Agentic AI SOC Platform that automates one of cybersecurity's most understaffed and time-intensive disciplines: detection engineering.

As cyber threats evolve faster than security teams can manually respond, organizations increasingly struggle to build, validate, tune, and maintain the detections needed to identify modern attacks. AI Detection Engineer continuously analyzes an organization's investigations,

threat hunting results, detection performance, and telemetry to identify coverage gaps, author new detections, optimize existing rules, and prioritize the improvements that will have the greatest impact on reducing organizational risk.



Prophet Security Dectection Engineer

Unlike traditional coverage dashboards that simply report which detection rules are enabled, AI Detection Engineer measures real-world detection effectiveness by analyzing completed investigations. The result is a continuously updated view of which MITRE ATT&CK techniques are effectively covered, which detections have gone quiet, and where dangerous blind spots remain.

“AI Detection Engineer gave us a real view of where our coverage actually stood, tuned our rules that were contributing to false positive noise, and proposed new detections it had already backtested against our own investigation data. That's work we simply didn't have the people or hours to do ourselves, and we decided how much autonomy to give it along the way," said Lisa Brooks, Director, Information Security - Security Operations & Engineering at ETS

From Reactive Detection to Continuous Detection Engineering
Detection engineering has become one of the fastest-growing priorities for security operations teams, yet few organizations have the specialized staff needed to continuously improve detection coverage. Detection engineers are routinely pulled into alert triage and incident response, leaving little time to analyze detection quality, tune existing rules, or identify new attack techniques before adversaries exploit them.

AI Detection Engineer continuously performs this work in the background, allowing security teams to wake up each day to a prioritized list of validated recommendations rather than months of untuned rules and unaddressed gaps.

Working from an organization's own investigation history, AI Detection Engineer:
 Builds a live MITRE ATT&CK coverage map based on investigation outcomes rather than static rule inventories.
 Identifies detection coverage gaps and telemetry blind spots across the environment.

- Authors new detections using the organization's existing security stack.
- Tunes existing detection rules to reduce false positives and analyst fatigue.
- Backtests every recommendation against historical data before proposing implementation.
- Maintains version control, documentation, audit trails, and rollback capabilities for every change.

Rather than replacing analysts, AI Detection Engineer automates the repetitive engineering work that most security teams lack the time and staffing to complete consistently.

AI That Earns Trust Through Transparency

Prophet designed AI Detection Engineer around a simple principle: organizations should determine how much autonomy AI receives.

Every recommendation includes supporting investigation evidence, an explanation of why the recommendation was generated, confidence scoring, and historical backtesting results before any change is implemented. Organizations can begin in Prophet's default review-and-approve mode or progressively allow greater automation as confidence grows.

Every recommendation remains fully documented, version controlled, and reversible, giving security teams the transparency and governance needed to adopt autonomous security operations responsibly.

"Security teams have known for years that detection engineering is essential, but they haven't had the people or the time to do it continuously," said Grant Oviatt, Co-Founder and Vice President of Product at Prophet Security. "AI Detection Engineer turns detection engineering from an occasional project into a continuous operational capability. Because Prophet AI performs the investigations, it understands which detections matter most, which gaps create the greatest risk, and where teams can make the biggest improvements. Organizations remain in complete control while AI handles the work that never seems to fit into the day."

Why This Matters

AI Detection Engineer extends the Prophet Agentic AI SOC Platform across the full security operations lifecycle, allowing organizations to automate:

- Alert triage
- Security investigations
- Threat hunting
- Detection engineering
- Continuous detection optimization

Together, these capabilities create an AI SOC Platform that not only investigates today's alerts but continuously improves tomorrow's detection coverage.

Availability

AI Detection Engineer is available immediately.
To learn more or request a demonstration, visit https://www.prophetsecurity.ai/ai-detection-engineer

About Prophet Security
Prophet Security's mission is to be a force multiplier for security teams by delivering a comprehensive Agentic AI SOC Platform that automates the manual processes across security operations - from alert triage, investigation and incident response to threat hunting, and detection engineering. Prophet AI reduces mean time to investigate, mean time to respond, and delivers a 10x increase in team productivity.The platform reduces risk by finding and closing the gaps in your detection coverage that let attackers operate undetected. Prophet Security's investors include Accel, Bain Capital Ventures, Amex Ventures and Citi Ventures. Learn more at prophetsecurity.ai.

FAQ
What is Prophet's AI Detection Engineer?
AI Detection Engineer is an AI-powered detection engineering capability that continuously identifies coverage gaps, authors new detections, tunes existing rules, validates recommendations through historical backtesting, and improves an organization's overall security posture.

How is AI Detection Engineer different from traditional SIEM rule management?
Traditional SIEM platforms primarily manage existing rules and inventories. AI Detection Engineer analyzes completed investigations and threat hunting results to determine which detections are effective, which have become stale, and where organizations have genuine blind spots.

Does AI automatically change detections?
No. Organizations choose the level of AI autonomy they want. Every recommendation can be reviewed, validated through backtesting, version controlled, approved, or rolled back before deployment.

Kari Ritacco
RedIron PR
kari@redironpr.com
Visit us on social media:
LinkedIn
X