Rapid7 Puts Agentic AI to Work in the SOC, Empowering Analysts to Investigate Smarter and Faster

2025-06-24

Agentic AI workflows transform managed detection & response (MDR), giving SOC analysts time to focus on higher-impact activities and customers better command of their attack surface with faster time-to-insight and improved alert fidelity

BOSTON, June 24, 2025 (GLOBE NEWSWIRE) -- Today, Rapid7, Inc. (NASDAQ: RPD), a leader in threat detection and exposure management, announced that agentic AI workflows are now embedded within Rapid7's next-gen SIEM and XDR platform to fundamentally change how threats in MDR customer environments are investigated in the SOC. Leveraging **Rapid7's AI Engine**, agentic AI autonomously performs foundational investigative tasks with the rigor and expertise of a SOC analyst, but at AI speeds. This empowers analysts to perform deeper analysis, shorten investigation cycles, and ultimately solve security problems faster for customers.

As AI **accelerates** the threat **landscape**, enabling attackers to launch faster, more personalized, and harder-to-detect campaigns, organizations need an MDR experience that scales to meet the demands of their environment and the broader attacker landscape while providing direct visibility into decisions. The new agentic AI workflows in Rapid7 MDR address the demand for scale, speed and transparency, incorporating Rapid7's industry-leading AI automation for alert triage, which closes benign alerts with 99.93% accuracy and saves 200+ SOC hours per week.

"AI isn't just an enhancement to security operations, it's a catalyst for a new era of scale, speed, and strategic decision-making. At Rapid7, we believe AI must be human-centric, transparent and accountable, and built on analyst expertise," said Laura Ellis, vice president of AI and data at Rapid7. "The launch of agentic AI workflows for MDR represents the foundational step in our broader vision for agentic AI across the platform. Far more than just

automation, this is the beginning of a system capable of intelligent and adaptive decision-making."

Agentic AI workflows are trained on playbooks designed by Rapid7's own SOC experts, and refined through continuous real-world application, ultimately **delivering**:

- Improved confidence in security postures through scalable, repeatable, high quality investigations that protect against sophisticated AI attackers amid increasing alert volume.
- Greater visibility and control of service outcomes with transparency into the reasoning, evidence, and logic behind every AI-powered action and output.
- Maximum return on detection and response investments via reallocation of analyst hours to the most complex tasks and strategic decisions to maximize impact across customer environments.

"A world-class SOC optimizes for the 'human' decision moment. With agentic AI workflows, we're using AI to present the right information to enable accurate and fast human decisions that allow organizations to quickly find and stop today's AI-enabled attackers," said Jon Hencinski, vice president detection & response at Rapid7. "Agentic AI workflows automate repetitive tasks, surface relevant findings, and provide contextual information to support analyst decision-making. By delivering timely, actionable insights, these workflows improve the quality of decisions being made and empower analysts to move confidently to the next step in the response process."

"Successful AI deployment in any cybersecurity platform needs to be thoughtful and planned: from the classification of data through to disciplined workflows and orchestration of detections with responses. Rapid7's approach to AI implementation checks each of these boxes with deliberate, transparent, practical AI processes that deliver real-world efficiencies for its customers," said Craig Robinson, research vice president at IDC.

To learn more about Rapid7's Managed Detection and Response service with agentic AI Workflows, visit **https://www.rapid7.com/services/managed-detection-and-response-mdr**.

About Rapid7
Rapid7, Inc. (NASDAQ: RPD) is on a mission to create a safer digital world by making cybersecurity simpler and more accessible. We empower security professionals to manage a modern attack surface through our best-in-class technology, leading-edge research, and broad, strategic expertise. Rapid7's comprehensive security solutions help more than 11,000 global customers unite cloud risk management with threat detection and response to reduce attack surfaces and eliminate threats with speed and precision. For more information, visit our **website**, check out our **blog**, or follow us on **LinkedIn** or **X**.

Rapid7 Media Relations

Alice Randall

Director, Global Communications

press@rapid7.com

(857) 216-7804

Rapid7 Investor Contact

Elizabeth Chwalk

Vice President, Investor Relations

investors@rapid7.com

(617) 865-4277

Source: Rapid7