



NEWS RELEASE

Rapid7 Launches Incident Command: AI-Native SIEM Empowers Analysts to Act with Speed and Precision from Risk to Response

2025-07-29

Powered by SOC-tested AI and built on the Command Platform's integrated data foundation, Incident Command delivers detection, automation, attack surface context, and threat intelligence in one SOC experience

BOSTON, July 29, 2025 (GLOBE NEWSWIRE) -- Today, **Rapid7, Inc.** (NASDAQ: RPD), a leader in threat detection and exposure management, announced the launch of **Incident Command**, a powerful new next-gen SIEM extending the capabilities of its **Command Platform**, purpose-built to transform how security teams detect, investigate, and respond to threats. Incident Command unifies preventative attack and exposure management together with threat detection and response, all powered by Agentic AI **workflows** trained on playbooks designed by Rapid7's own SOC experts, and refined through continuous real-world application.

Built on the Command Platform's data mesh, Incident Command brings attack surface context through **Surface Command** and curated threat intelligence with **Intelligence Hub** to deliver a **seamless user experience** that enables every analyst to operate like an expert, every action to be informed by context, and every response to be faster, smarter, and simpler.

"The launch of Incident Command is a leap toward our mission to simplify access to security outcomes," said Corey Thomas, CEO of Rapid7. "Security teams are under scrutiny to deliver measurable impact across their risk and response programs. We built the Command Platform to unify all customer data—not just what we collect—so that organizations get the facts from the beginning and reduce their time to action. Incident Command, our upgraded next-gen SIEM, gives customers the benefit of the Command Platform plus broadened access to our decades of SOC expertise with agentic AI integrated within the workflows they use every day."

With Incident Command, security teams operate within a closed-loop feedback model, combining AI-powered threat detection with deep exposure visibility, automating triage with 99.93% accuracy, and saving 200+ SOC hours per week. Key features of **Incident Command** include:

- Agentic AI, built by and for the SOC: Unlike black-box “AI” tools, Rapid7’s AI is trained on years of detection, investigation, and response data from its 24/7 MDR operations, enabling transparent, analyst-assistive triage and investigation workflows with 99.93% benign disposition accuracy. It doesn’t just classify, it guides, recommends, and adapts with every use.
- Unified analyst experience: Incident Command brings together historically siloed SIEM, SOAR, ASM, and threat intelligence functions into one intuitive interface. Analysts can investigate with deep threat, exposure, and asset context in a single view—no context switching required.
- Open and integrated data mesh: Powered by Surface Command and the Command Platform’s data mesh, customers can unify Rapid7 and third-party telemetry without complex integrations, gaining end-to-end visibility across their hybrid environments.
- Deeply embedded threat intelligence: Expertly vetted threat intelligence is integrated within Incident Command for the most actionable, relevant, and context-rich insights for targeted detection, threat hunts, and incident response.

“With Incident Command, Rapid7 is marrying exposure management capabilities with threat detection and this is a differentiator in a crowded SIEM market,” said Michelle Abraham, senior research director at IDC. “By bringing detection automation, internal and external attack surface visibility, threat intelligence, and AI automation into one platform, Rapid7 is offering security analysts a solution that reduces complexity, connects data, and streamlines investigations, which improves analyst workflows.”

To learn more about Incident Command, visit <https://www.rapid7.com/products/siem/>.

Rapid7 is showcasing Incident Command at Black Hat USA, August 6-7 in Las Vegas, both in the Business Hall (Booth #5042) and at The Border Grill in Mandalay Bay from 9am - 6pm on August 6. Click **here** to learn more and sign up for a demonstration.

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