NEWS RELEASE

Rapid7 InsightIDR Successfully Completes The Latest MITRE Engenuity ATT&CK Enterprise Evaluation

3/31/2022

Demonstrates Strong Signal-to-Noise Across the Attack Chain in Emulation of Wizard Spider and Sandworm Threat Groups

BOSTON, March 31, 2022 (GLOBE NEWSWIRE) -- **Rapid7, Inc.** (Nasdaq: RPD), a leading provider of security analytics and automation, today announced the results of its completed 2022 MITRE Engenuity ATT&CK® Evaluation of Rapid7 **InsightIDR** and the Insight Agent. This round of independent **ATT&CK Evaluations** for enterprise cybersecurity solutions emulated the Wizard Spider and Sandworm threat groups. Rapid7's InsightIDR and Insight Agent demonstrated strong signal-to-noise across the attack chain during these simulations.

InsightIDR is Rapid7's industry-leading cloud SIEM and Extended Detection and Response (XDR) offering, and the included Insight Agent provides coverage across assets—in the cloud or on-premises—and powers InsightIDR's endpoint detection and response (EDR) capabilities. The MITRE ATT&CK evaluation results showcase high-fidelity detections unlocked with InsightIDR and the Insight Agent. InsightIDR demonstrated consistent ability to detect threats early in the cyber kill chain, strong signal-to-noise, and solid visibility across the ATT&CK Framework, identifying telemetry, tactics, or techniques across 18 of the 19 phases presented in the attack simulations. The detections in this evaluation represent a small segment of the InsightIDR detections library, which provides native telemetry and high-fidelity detections across networks, users, and clouds in addition to endpoints—all vetted in the field by Rapid7's managed detection and response (MDR) security operations center analysts to ensure relevancy and actionability for InsightIDR customers.

MITRE ATT&CK Evaluations prioritize threats that offer unique impact to businesses and governments worldwide. Through the lens of the ATT&CK knowledge base, the 2022 MITRE ATT&CK evaluations focused on two threat actors: Wizard Spider and Sandworm. **Wizard Spider** is a financially motivated criminal group that has been

conducting ransomware campaigns since August 2018 against a variety of organizations, ranging from major corporations to hospitals. **Sandworm** is a destructive Russian threat group that is known for carrying out notable attacks such as the 2015 and 2016 targeting of Ukrainian electrical companies and NotPetya attacks in 2017. MITRE chose Wizard Spider and Sandworm threat actors based on their complexity, relevancy to the market, and MITRE Engenuity's ability to emulate the adversary.

"This MITRE ATT&CK evaluation demonstrates the high-fidelity detections that customers value with InsightIDR," said Sam Adams, Vice President of Detection and Response, Rapid7. "From our own MDR service, we understand firsthand the importance of having a comprehensive, relevant, and reliable detection set that customers can trust. InsightIDR's native EDR capabilities highlighted in this evaluation are just one example of how we help customers get there."

"This latest round indicates significant product growth from our vendor participants. We are seeing greater emphasis in threat-informed defense capabilities, which in turn has developed the infosec community's emphasis on prioritizing the ATT&CK Framework," said Ashwin Radhakrishnan, acting General Manager of ATT&CK Evaluations at MITRE Engenuity.

Rapid7 believes an open security community, data-sharing projects, research, and testing are fundamental to driving continuous improvement. All of these helped InsightIDR—and the Insight Agent that powers its EDR capabilities—evolve into a leading cloud-based SIEM, and is now ushering in the next era of detection and response with XDR.

With **InsightIDR**'s endpoint capabilities security professionals can:

- Unlock real-time monitoring for both on-premises and remote endpoints, and a vast library of critical attacker behavior and endpoint detections—all mapped in detail to the MITRE ATT&CK framework
- Bait attackers and address areas of exposure with honey credentials deployed by the agent, helping identify intruders on- or off-network
- Access enhanced endpoint telemetry—for custom detection, investigations, threat hunting, and forensics
- Achieve faster mean-time-to-respond (MTTR) with automated containment leveraging the Insight Agent with InsightIDR and its security orchestration, automation and response (SOAR) capabilities

To learn more about InsightIDR and the Insight Agent, visit the **Rapid7 blog**.

The Evals team chose to emulate two threat groups that abuse the **Data Encrypted For Impact (T1486)** technique. In Wizard Spider's case, they have leveraged data encryption for ransomware, including the widely known **Ryuk malware (S0446)**. Sandworm, on the other hand, leveraged encryption for the destruction of data, perhaps most

notably with their **NotPetya malware (S0368)** that disguised itself as ransomware. While the common thread to this year's evaluations is "Data Encrypted for Impact," both groups have substantial reporting on a broad range of post-exploitation tradecraft.

About MITRE Engenuity

MITRE Engenuity, a subsidiary of MITRE, is a tech foundation for the public good. MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE Engenuity brings MITRE's deep technical know-how and systems thinking to the private sector to solve complex challenges that government alone cannot solve. MITRE Engenuity catalyzes the collective R&D strength of the broader U.S. federal government, academia, and private sector to tackle national and global challenges, such as protecting critical infrastructure, creating a resilient semiconductor ecosystem, building a genomics center for public good, accelerating use case innovation in 5G, and democratizing threat-informed cyber defense.

For full results and more information about the MITRE evaluations, please visit: **https://attackevals.mitre-engenuity.org/enterprise/wizard-spider-and-sandworm/**.

About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Over 10,000 customers rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. For more information, visit our **website**, check out our **blog**, or follow us on **LinkedIn** or **Twitter**.

Press contact:
Kelly Crummey
Corporate Communications
press@rapid7.com
(617) 921-8089

Investor contact:
Sunil Shah
Vice President, Investor Relations
investors@rapid7.com

(617) 865-4277

Source: Rapid7