Resilient, an IBM Company Helps Organizations Respond to and Manage Ransomware
Wednesday, December 14, 2016 11:00:00 AM (GMT)

CAMBRIDGE, Mass., Dec. 14, 2016 /PRNewswire/ -- Resilient, an IBM Company (NYSE: IBM) today released the industry's first Dynamic Playbook for ransomware, aimed at helping organizations globally respond effectively to this growing type of cyberattack. Dynamic Playbooks, the latest innovation to Resilient's Incident Response Platform, automate and orchestrate, in real-time, the variety of actions organizations need to take in response to cyberattacks.

According to a new IBM (NYSE: IBM) study, seven out of 10 U.S. businesses surveyed infected with ransomware have paid to resolve a ransomware attack, with more than half paying more than $10,000. To help organizations respond rapidly and strategically to this type of threat and many other types of threats, Resilient's new Dynamic Playbooks are an industry first in the incident response management market. Resilient's Dynamic Playbooks provide an unmatched orchestration of incident response by adapting in real-time to the details of a cyberattack or other business threat, and enabling effective, rapid response to more sophisticated threat types.

"Fast-moving, sophisticated threats like ransomware require new and actively adaptive response methods. Resilient's Dynamic Playbooks set another new standard for agility, intelligence, and sophistication in the battle to respond to and recover from today's complex cyber threats," said John Bruce, CEO and Co-Founder of Resilient, an IBM Company. "Ransomware is just one example of the cyberattacks facing companies today, but its growing rate of prevalence is threatening businesses like never before. This technology arms companies with a response approach that manages the intensity of the problem."

Resilient's Dynamic Playbooks share several critical and differentiating attributes:

- Agile: Resilient's Dynamic Playbooks continually react to changes by leveraging rules and scripts that implement business logic and enriching incidents as they progress.
- Intelligent: By leveraging information from other connected systems, Dynamic Playbooks make rules-based decisions to take actions – such as increasing priority or involving other parts of the organization, such as legal. By the time an analyst opens an incident, many repetitive, initial triage steps have already been completed.
- Sophisticated: Dynamic Playbooks keep business rules separate from workflows, eliminating the need for a proliferation of static playbooks with only slight variations, and keeping management overhead to a minimum.

As an example of how this works, consider a spear-phishing attack on a work laptop used by a senior executive. Before an analyst in the security operations center even sees the incident, rules and conditions associated with the Dynamic Playbook have used information from connected systems to determine that the user is an executive, automatically escalated the alert to tier-2 analysts, raised the official severity code for the incident, and notified the company's legal team.

In addition, Resilient's Dynamic Playbooks support integrations with more than 100 other systems that may be present in a typical security environment, providing Resilient clients with a seamless, centralized incident response hub. Built for security leaders by security leaders, Resilient's Incident Response Platform processes more than 1 million incidents a day.

The State of Cyber Resilience in 2016
The state of Cyber Resilience among U.S. businesses has not improved in the past year. According to the Ponemon Institute 2016 State of Cyber Resilience study sponsored by Resilient, only 32 percent of IT and security professionals say their organization has a high level of Cyber Resilience – down slightly from 35 percent in 2015. Seven out of 10 spend the same or more time dealing with a cyber incident than a year ago, and more than half say their leaders don't recognize the link between cyber resilience and revenues or brand reputation. At the same time, what has increased over the past year is the average cost of a data breach -- now estimated at $4 million per incident.

The greatest barriers to Cyber Resilience among U.S. organizations are:

- Insufficient planning and preparedness
- Complexity of business processes
- Insufficient risk awareness, analysis and assessments
- Complexity of IT processes
- Silos and turf issues

To download the 2016 Cyber Resilient Organization study, visit http://info.resilientsystems.com/ponemon-institute-study-the-2016-cyber-resilient-organization. To view the infographic, follow this link.

About Resilient, an IBM Company
Resilient's mission is to help organizations thrive in the face of any cyberattack or business crisis. The industry's leading Incident Response Platform (IRP) empowers security teams to analyze, respond to and mitigate incidents faster, smarter and more efficiently. Part of IBM Security, the Resilient IRP also integrates security technologies into a single hub and provides an orchestrated workflow spanning an organizations people, process and technology driving down response time. With Resilient, security teams can have best-in-class response capabilities. Resilient has more than 130 global customers, including 30 of the Fortune 500 and partners in more than 20 countries. Learn more www.resilientsystems.com.

About IBM Security
IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors more than 35 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Contacts:

Dan Kloeffler
Vice President, Senior Media Specialist, Ketchum
646-935-4036
dan.kloeffler@ketchum.com

Kelly Kane
IBM Security
413-297-2668
kkane@us.ibm.com

To view the original version on PR Newswire, visit:http://www.prnewswire.com/news-releases/resilient-an-ibm-company-helps-organizations-respond-to-and-manage-ransomware-300377871.html

SOURCE IBM

Countries: United States
Industries: Computer Electronics, Hardware & Software, High Tech Security, Multimedia, Internet & Wireless Technology
Languages: English
Primary Identifiers: IBM-US
Related Identifiers: IBM-US
Subjects: New Products & Services