May 31, 2017

Security Teams Overwhelmed by Rising Volume of Attacks

New Research Finds "Time Sink" Security Investigation Threatens Effective Security Operations

SAN FRANCISCO--(BUSINESS WIRE)-- Splunk Inc. (NASDAQ: SPLK), provider of the leading software platform for real-time Operational Intelligence, today announced the results of new research from IDC that shows organizations are constantly under attack and struggling to keep up. The research finds most organizations run time-consuming security investigations and often fail to effectively protect themselves. Read the full IDC InfoBrief, "Investigation or Exasperation? The State of Security Operations," sponsored by Splunk.

Findings from a survey of 600 senior security professionals across the U.S. and Europe highlight that less than half (47 percent) of security teams gather enough information about those incidents to enable appropriate or decisive action. Firms experience an average of 40 actionable incidents per week, but only a quarter (27 percent) think they are coping comfortably with this workload, and a third (33 percent) describe themselves as "struggling" or "constantly firefighting." More than half (53 percent) of respondents claimed the biggest limitation to improving security capabilities was that resources are too busy on routine operations and incident investigation.

"The amount of time companies are spending on analyzing and assessing incidents is a huge problem," said Duncan Brown, associate vice president, security practice, IDC. "The highest-paid, most skilled staff are being tied up, impacting the cost and efficiency of security operations. This is exacerbated when considered alongside the security skills shortage, which has most impact in high-value areas like incident investigation and response. Organizations must ensure that they are using their data effectively to gain key insights quickly to determine cause and minimize impact."

"It's time to change how we approach incident response," said Haiyan Song, senior vice president, security markets, Splunk. "As attacks become more advanced, frequent, and take advantage of IT complexity, we must become proactive in our approach to security - how else will we know we have been breached? As demonstrated by the swift, global spread of WannaCry, it has never been more important for organizations to proactively monitor, analyze and investigate to verify whether there are real threats, then prioritize and remediate the most critical. By taking an analytics-driven approach, and increasingly automating when possible, security teams can shorten investigation cycles, respond quickly and appropriately in the event of a compromise, free up resources to focus on more strategic initiatives and ultimately improve security posture."

Other findings from the study include:

- **Everyone's under attack.** 62 percent of firms are being attacked at least weekly, with 30 percent attacked daily and 10 percent hourly or continuously. 45 percent are experiencing a rise in the number of security threats.
- **The volume of incidents is challenging.** Organizations experience an average of 40 actionable security alerts per week, with this number rising to 77 for finance and 124 for telco.
- **Most firms only surface a breach to the board at the last possible moment**. Asked when they report a security incident to the board, the top triggers were sensitive data breach (66 percent), compromised customer data (57 percent), and a mandated notification to a regulator (52 percent). Only 35 percent of firms have breach reporting to the board built into their defined incident response processes.

To find out how you compare to your peers when it comes to incident response, visit IDC's Security Response Readiness Assessment.

Methodology

IDC surveyed 600 global organizations with over 500 employees in the U.S., U.K., Germany, France, Sweden and the Netherlands.

The full IDC InfoBrief can be downloaded here.

About Splunk Inc.

Splunk Inc. (NASDAQ: SPLK) is the market leader in analyzing machine data to deliver Operational Intelligence for security, IT and the business. Splunk® software provides the enterprise machine data fabric that drives digital transformation. More than 13,000 customers in over 110 countries use Splunk solutions in the cloud and on-premises. Join millions of passionate users by trying Splunk software for free: http://www.splunk.com/free-trials.

Social Media: Twitter | LinkedIn | YouTube | Facebook

View source version on businesswire.com: http://www.businesswire.com/news/home/20170531005356/en/

Media
Splunk Inc.
Bill Bode, 415-266-3994
bbode@splunk.com
Alice Crook, +44 (0)20 3204 4353
acrook@splunk.com
or
Investors
Splunk Inc.
Ken Tinsley, 415-848-8476
ktinsley@splunk.com

Source: Splunk Inc.

News Provided by Acquire Media