



FOR IMMEDIATE RELEASE

Contact:

Amy Pasquarello

703-883-9000, ext. 146

apasquarello@meritalk.com

CYBER THREATS LIVE ON GOVERNMENT NETWORKS FOR AVERAGE OF 16 DAYS BEFORE THEY ARE DETECTED

86 percent of government cyber pros say big data analytics will help

Alexandria, Va., April 28, 2015 – [MeriTalk](#), a public-private partnership focused on improving the outcomes of government IT, today announced the results of its new report, “[Go Big Security](#),” underwritten by [Splunk Inc.](#) The study finds that government cyber security professionals estimate that cyber threats exist on their networks for an average of 16 days before they are detected – hiding in plain sight. The good news is that 86 percent say big data analytics will improve cyber security efforts. But, just 28 percent are fully leveraging big data for security purposes today. The report examines the state of cyber security in Federal, state and local government agencies, and identifies steps to empower these organizations to make the shift from compliance to risk management to see better security outcomes.

Government cyber security professionals say big data can help make cyber security risk management more effective and proactive. Today, nine out of 10 respondents say they cannot tell a “complete story” with the cyber security data they receive. As a result, 76 percent of cyber security professionals say their security team often operates reactively rather than proactively.

By leveraging big data and analytics, government cyber security professionals say they could better detect a breach that is in process (61percent), monitor streams of data in real time (51 percent), and conduct a conclusive root-cause analysis following a breach (49 percent). Yet, just one in three say they are prioritizing big data analytics for cyber security – why’s big data on the bench?

“Government organizations have access to a wealth of cyber threat information,” says Kevin Davis, area vice president, Public Sector, Splunk. “The challenge is managing that data and

connecting the dots in real time. That’s how we get immediate insight into threats. Agencies need to detect threats faster and start to predict when and how they will occur.”

There are challenges. Organizations are drowning in data – 68 percent say their organization is overwhelmed by the volume of security data. Forty-five percent of Federal IT managers cite data volume as the biggest challenge when it comes to fully leveraging big data analytics for cyber security, while 54 percent of state and local government IT managers cite lack of resources, specifically skilled personnel. Additionally, 78 percent of all government cyber security professionals say at least some of their security data goes unanalyzed due to a lack of time and/or skill of their team. And, while 70 percent say their organization can monitor streams of cyber data in real time, fewer can analyze it – of the security capabilities identified by respondents, statistical analysis is the weakest area.

“Moving from compliance to risk management is a mindset shift,” says Steve O’Keeffe, founder, MeriTalk. “Agencies need to think about ‘big security’ alongside big data. CDOs need to be on the court. Data is the MVP.”

Government cyber security professionals believe they need management support, funding, and training to move to a more proactive cyber security strategy and leverage security data to the fullest. They are making positive strides – 92 percent are working to improve cyber security – investing/upgrading existing security technologies (65 percent), deploying network analysis and visibility solutions (51 percent), and investing in training (50 percent).

The “Go Big Security” report is based on an online survey of 302 Federal, state and local government cyber security professionals in March 2015. The report has a margin of error of +/- 5.6 percent at a 95 percent confidence level. To download the full study, please visit:

www.meritalk.com/go-big-security.

About MeriTalk

The voice of tomorrow’s government today, MeriTalk is a public-private partnership focused on improving the outcomes of government IT. Focusing on government’s hot-button issues, MeriTalk hosts [Big Data Exchange](#), [Cloud Computing Exchange](#), [Cyber Security Exchange](#), and [Data Center Exchange](#) – platforms dedicated to supporting public-private dialogue and collaboration. MeriTalk connects with an audience of 85,000 government community contacts. For

more information, visit www.meritalk.com or follow us on Twitter, @meritalk. MeriTalk is a [300Brand organization](#).

About Splunk Inc.

Splunk Inc. (NASDAQ: SPLK) provides the leading software platform for real-time Operational Intelligence. Splunk® software and cloud services enable organizations to search, monitor, analyze and visualize machine-generated big data coming from websites, applications, servers, networks, sensors and mobile devices. More than 9,000 enterprises, government agencies, universities and service providers in more than 100 countries use Splunk software to deepen business and customer understanding, mitigate cybersecurity risk, prevent fraud, improve service performance and reduce cost. Splunk products include Splunk® Enterprise, Splunk Cloud™, Hunk®, Splunk MINT Express™ and premium Splunk Apps. To learn more, please visit <http://www.splunk.com/company>.