MeriTalk
Improving the Outcomes of Government IT

Contact:
Sarah Masuda
703-883-9000 ext. 126
smasuda@meritalk.com

Feds Can Save More Than $5 Billion Annually and Act Faster by Improving Threat Monitoring, Correlation, and Automation of Protections

New Study Highlights Need for Actionable Cyber Awareness

Alexandria, Va., November 14, 2016 – MeriTalk, a public-private partnership focused on improving the outcomes of government IT, today announced the findings of its latest report, "Pedal to the Metal: Mitigating New Threats Faster with Rapid Intel and Automation." The report, underwritten by Palo Alto Networks, reveals feds can save up to 27 percent – or $5 billion annually – of their cybersecurity budget and address threats faster by improving threat monitoring, correlation, and protection automation.

Our networks are radically changing – we're moving to the cloud, going mobile, and using SaaS applications as never before. Our security approach needs to adapt to address this shift. According to the report, agencies may be missing key indicators of an attack – a pathway into their networks – and unable to correlate threat data points. While the majority of agencies monitor traditional entry points (such as mail servers, the web, and internet gateways), the report found that fewer than half guard data centers (north/south and east/west), SaaS enforcement points, and mobile endpoints. This may impede the organization's ability to spot discrete malicious behaviors.

Even with the enforcement points that are being monitored, only a little over half (61 percent) of agencies are capable of automatically distributing information against malicious behaviors across different enforcement points.

Timing is critical, given how fast threats spread within the networks. When it's time to take swift action, only 15 percent say their agency can create protections against a new threat within a few minutes – and only 17 percent can distribute these protections for enforcement within that same brief time frame.

Organizations share threat feeds today with the aspiration that these insights will help them prevent new threats on their own networks. Feds subscribe to a daunting amount of threat feeds daily, ingesting an average of such 25 external feeds daily, the report found. Almost half are received via email, drastically increasing the time it takes to distribute new protections based on those insights. Seventy-two percent say it takes a few hours to a few days to assess if a unique threat is

(more)

present and determine if action is required. Eighty-one percent also state it takes just as long to create actionable changes in their organization's security posture.

Despite these time-intensive processes, federal security operations teams continue to allocate precious manpower and financial resources to tasks that can be automated. Twenty percent of security operations professionals say 12 or more members of their agency's security operations center (SOC) team are primarily responsible for:

- Creation of custom signatures for security technologies on the network
- Correlation of isolated network events that may be related to part of a campaign
- Taking threat intelligence from various feeds and making it actionable
- Correlating different behaviors (IOCs) to associate them with one or more threat campaigns

"To address today's threats and prevent successful cyberattacks, it's imperative to automate the creation and distribution of new protections in near-real time and predict the attacker's next step," said Pamela Warren, director of government and industry initiatives, Palo Alto Networks. "To do this, you need the data, the tools and the process. The survey indicates feds have plenty of data, but need to implement the tools and the processes to achieve that goal."

Additionally, the report found that many security operations professionals are not utilizing critical advanced threat capabilities. Seventy-one percent of agencies use some form of automated analysis and reports to reduce the volume of data and focus efforts on hunting targeted attacks. However, fewer than half use advanced techniques – specifically, dynamic analysis (48 percent), static analysis (32 percent), and machine learning (19 percent) – which, working together, improve threat analysis and the ability to anticipate future threats.

Despite the need for the automation of prevention, only 30 percent of federal security operations professionals are willing to invest in the automation of signature creation and distribution.

"Agencies are falling into a culture that's too focused on the legacy, manual way of doing security," says Steve O'Keeffe, founder, MeriTalk. "Feds need their technology investments – not just their human expertise – to detect new attacks and determine what's a full-blown, global, coordinated campaign as opposed to an unrelated or one-time event – and act accordingly to quickly and effectively minimize damage."

For agencies to assess threats as quickly and efficiently as possible, the report outlines the following recommendations:

- Ensure detection and enforcement across all potential attack vectors into the network to detect any anomalies that could be new threats.
- Correlate isolated tactical behaviors as a sign of a bigger attack pattern, as well as isolate network segments to reduce the effectiveness of attacks.

- Prevent new attacks by first analyzing and accurately predicting the next step in the attack (location and behavior) before it occurs.
- Leverage new techniques, like machine learning, dynamic and static analysis, in conjunction. Then, swiftly create new protection and reprogram enforcement points faster than the attack can spread in the network.

The "Pedal to the Metal" report is based on an online survey in September 2016 of 150 federal employees who work with their security operations team. The report has a margin of error of ±7.97 percent at a 95 percent confidence level. To download the full study please visit: https://www.meritalk.com/study/pedal-to-the-metal/.

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 115,000 government community contacts. For more information, visit www.meritalk.com or follow us on Twitter, @meritalk. MeriTalk is a 300Brand organization.