FOR IMMEDIATE RELEASE

Contact: Star VanderHaar
Arketi Group for DefenseStorm
O: 404.929.0091 ext 206
M: 404.822.6819
F: 404.321.3397
svanderhaar@arketi.com

DefenseStorm Chief Information Security Officer Reveals How to Affordably Protect Against Cyber Bad Actors At InfoSec World 2018

-- Cybersecurity expert Robert Thibodeaux outlines best practices at 10:00 a.m. ET Monday, March 19 --

ORLANDO, Fla., and ALPHARETTA, Ga. (March 14, 2018) – In a session titled "Detecting Internal Threat Actors Without Breaking the Bank," at InfoSec World 2018, DefenseStorm Chief Information Security Officer Robert Thibodeaux will highlight strategies for defending against cyber threat actors that have compromised an endpoint and have pivoted to collecting insider credentials and other information. InfoSec World 2018 Conference and Expo, the longest running conference dedicated to the business of information security, expects to draw more than 1,000 information security professionals representing 14 countries March 19 – 21 at Disney's Contemporary Resort in Lake Buena Vista, Florida.

A 2018 Security Threat Landscape presentation by research firm Gartner noted that despite 20 billion threat blocks per day, IT infrastructures continue to become more vulnerable with advances in the complexity and heterogeneity of endpoints, systems, applications and data. Thibodeaux advises organizations to detect and block what threats they can, but also to continually assume they have been breached and take the next step of "turning on the light" within their internal infrastructure.

On most production networks, a lack of instrumentation on endpoints, servers and networking infrastructure makes it difficult to detect threat actors that have intruded an organization to begin harvesting credentials and other information. While most businesses invest in Security Information and Event Management (SIEM) software, many do not have instrumentation that detects malicious activity on endpoints when malware is not being used. Thibodeaux reveals best practices, along with free or inexpensive tools, that organizations can use to get richer log data and indicators of attack and compromise into the SIEM for incident responders to detect and interdict.

"Bob's cybersecurity expertise is an invaluable resource for the regional and community-focused banks and credit unions we serve," said DefenseStorm Chief Executive Officer Sean Feeney. "His instructional and practical approach to helping organizations assess their vulnerabilities and execute protective measures is part of the added personalized value we deliver to customers," he added.

Thibodeaux has more than 20 years of experience as a senior security expert and accomplished IT executive and engineer. Through leadership positions managing IT departments and programs, technology operations and data centers, he has driven innovative process improvements, disaster recovery programs, information security strategies, and audit and compliance improvements. He has been responsible for incident response, risk management and penetration testing for community-focused banks, credit unions and high-tech companies across the United States, and serves as Chief Information Security Officer for DefenseStorm, the only company that combines and automates together in real time cybersecurity and cybercompliance built for banking. Thibodeaux is a Certified Information Systems Security Professional, Digital Forensics Examiner and GIAC Penetration Tester.

About DefenseStorm

DefenseStorm is the only company that combines and automates in real time cybersecurity and cybercompliance built for banking, so financial institutions can achieve Cyber Safety & Soundness according to regulations and their own policies. The DefenseStorm GRID™ is the only co-managed, cloud-based and compliance-automated solution of its kind, operating as a technology system and as a service supported by experts in financial institution security and compliance. It watches everything on an FI's network and matches it to defined policies for real time and proactive cyber exposure readiness. The FFIEC CAT requirements are built-in to an Active Compliance™ engine and automated, as can be other frameworks and an FI's own policies, turning manual "check-box" compliance into a real time discipline that meaningfully enhances an FI's risk management posture. A Threat Ready Active Compliance (TRAC) Team™ co-manages the DefenseStorm GRID with customers to deliver the advantages of a Security Operations Center in the cloud without adding staff and capital expenditures. www.DefenseStorm.com.

About InfoSec World Conference and Expo

For more than 20 years security professionals have made InfoSec World the "business of security" conference. Produced by MIS Training Institute (MISTI), InfoSec World assembles information security professionals from every market and field of study, from more than 100 nations. For more information on the conference, its detailed agenda as well as logistics, please visit: https://infosecworld.misti.com.

##