Stamus Networks Enhances Evidence Collection, Expands Threat Detection and Hunting, and Streamlines User Experience for Cyber Defenders

The latest update to the Stamus Security Platform (U39) is now generally available

INTERNATIONAL CYBERSECURITY FORUM (FIC) LILLE, FRANCE, April 5, 2023 – Stamus Networks, the global leader in Suricata-based network security, today announced the general availability of its latest software release, Update 39 (U39). The new release represents a significant enhancement to the company's flagship Stamus Security Platform (SSP), arming enterprise cybersecurity defenders with greater visibility while reducing the time it takes to respond to threats.

Trusted by security teams in the world's largest organizations, including government computer emergency response teams (CERTs), central banks, insurance providers, managed security service providers (MSSPs), multinational government institutions, broadcasters, travel and hospitality companies, and even a market-leading cybersecurity SaaS vendor, Stamus Security Platform helps defenders expose serious threats and unauthorized activity hidden in their networks.

U39 enhancements include:

- **Enhanced evidence collection** - new conditional packet capture (PCAP), protocol transaction, and flow logging give users additional evidence without excessive storage. Also, SSP now logs additional DCERPC, HTTP header, and TLS cipher suite metadata with each detection event (alert), giving users access to more complete metadata evidence during incident investigation and helping uncover hidden anomalies in a proactive threat hunt.
- **Expanded threat detection and hunting** - with U39, SSP users now have access to 21 new guided threat hunting filters and additional sources of threat intelligence, including 2 lateral movement rulesets and 3 suspicious domain lists. SSP can now detect activity from a match on the media type (also known as mime-type) and can ingest additional third-party threat intelligence feeds to trigger a detection event based on a match on IP addresses and domain lists.
- **Streamlined user experience** - the newly integrated threat hunting console offers an enhanced user experience by enabling seamless navigation from notifications to investigations, without compromising crucial contextual data. Users can now quickly and easily pivot between tasks, allowing for a more efficient process. Expanded Host Insights™ allows users to more rapidly identify all activity associated with a given host.

Stamus Networks will be demonstrating the latest version of Stamus Security Platform this week at the International Cybersecurity Forum (FIC stand G15) in Lille, France.

“Serious enterprise security practitioners need all the details, they want control, and they seek the truth about their network activity – wherever it leads them,” said Ken Gramley, CEO at Stamus Networks. “It's precisely these experts who have come to know and love SSP. We're thrilled to be able to bring this additional expert-level functionality to these cyber heroes.”

The unique power of the Stamus Security Platform derives from its consolidating three network security products into a single solution. By incorporating the very best features of intrusion detection (IDS), network security monitoring (NSM), and network detection and response (NDR) into Stamus Security Platform, security teams can reduce tool sprawl and meet their governance, risk, compliance, and operational security challenges with a single consolidated solution.

To learn more about the Stamus Security Platform, visit the Stamus Networks website at https://www.stamus-networks.com/stamus-security-platform

About Stamus Networks

Stamus Networks believes in a world where defenders are heroes, and a future where those they protect remain safe. As organizations face threats from well-funded adversaries, we relentlessly pursue solutions that make the defender’s job easier and more impactful. The global leader in Suricata-based network security solutions, Stamus Networks helps enterprise security teams know more, respond sooner and mitigate their risk with insights gathered from cloud and on-premise network activity. Our Stamus Security Platform combines the best of intrusion detection (IDS), network security monitoring (NSM), and network detection and response (NDR) systems into a single system that exposes serious and imminent threats to critical assets and empowers rapid response. For more information visit: stamus-networks.com.

###

Media Inquiries for Stamus Networks:
Kim Schofield
+1 (602) 234-4000
kim@stamus-networks.com