Stamus Networks Announces General Availability of New Software Release

Latest release brings powerful new detection and visualization capabilities to company's network detection and response (NDR) system

INDIANAPOLIS, USA and PARIS, FRANCE, June 10, 2021 – Stamus Networks, a global provider of high-performance network-based threat detection and response systems, today announced the availability of its latest software release, *Upgrade 37* (U37). The new release, which includes updates to both Stamus Network Detection (ND) and Stamus Network Detection and Response (NDR), gives cyber defenders a substantial set of new features along with a number of performance enhancements.

"This new release is a direct response to valuable input from our incredibly engaged customers who share our passion for an open, transparent and useful network detection and response solution," said Ken Gramley, CEO of Stamus Networks. "In addition to powerful new detection methods and response visualizations, we added capabilities specifically for the Suricata community and our managed security service provider (MSSP) partners."

The new features in U37 include the following:

- **Advanced threat timeline display** - improves visibility and transparency into the sequence of events that led up to a high-fidelity declaration of compromise™ by Stamus NDR.
- **Dynamic datasets** - continuously evaluates connections and traffic patterns for DNS server requests, encrypted connections, hosts, HTTP user agents, usernames, and other protocol attributes in order to identify new values, not encountered before.
- **Additional encrypted traffic metadata** - identifies and correlates TLS Server/Client pair using the JA3S algorithm to detect common infrastructure and command and control communications.
- **Automated alert triage and advanced NDR for native Suricata sensors** - extends key capabilities that were previously only available with Stamus Network Probes to Suricata users.
- **Embedded Cyberchef toolset** - builds on the suite of third-party tools available to the user under a single pane of glass by embedding Cyberchef directly into Stamus Security Platform (SSP).
- **Per-tenant webhooks** - allows managed security service providers to isolate integrations with client SOAR or messaging systems via individual webhook connections for each tenant.

- **Enhanced role-based access control** - improves organizations' ability to manage access to various SSP functions.

To learn more about the new capabilities of the Stamus family of network security products, read the blog article on the Stamus Networks website: https://www.stamus-networks.com/blog/release-u37

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. A global provider of high-performance network-based threat detection and response systems, 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 solutions are advanced network detection and response systems that expose serious and imminent threats to critical assets and empower rapid response. For more information visit: stamus-networks.com.

###

Media Inquiries:
D. Mark Durrett
+1 (919) 345-9515
mdurrett@stamus-networks.com