Stamus Networks Releases Latest Edition of Stamus Security Platform

Cyber Defenders Now Have Access to Powerful New Network-Based Attack Surface Visibility, Threat Detection, and Reporting Capabilities

INDIANAPOLIS and PARIS – August 1, 2024 – Stamus Networks, a global provider of high-performance network-based threat detection and response (NDR) systems, today announced that the latest edition (U40) of its Stamus Security Platform™ is now generally available. The company's flagship NDR system now boasts new attack surface visibility, threat and policy violation detection, and reporting capabilities that empower cyber defenders to succeed in the face of rising and increasingly sophisticated threats.

The power of the Stamus Security Platform comes from its multi-layered threat detection, hybrid network visibility, highly accurate automated response triggers, and open and transparent approach, which delivers explainable results backed up by extensive evidence.

Because no single technology can detect all threats, Stamus Networks incorporates not only artificial intelligence (AI) and statistical anomaly detection, but also traditional signatures and indicators of compromise (IoC) detection coupled with advanced noise reduction mechanisms. As such, it can effectively replace legacy intrusion detection systems (IDS), network security monitoring (NSM) systems, and first generation NDR systems, as it surpasses the baseline capabilities of today's typical NDR.

The Stamus Security Platform is a new generation of network-based security monitoring that gives cyber defenders detection they can trust with results they can explain.

Key enhancements of U40 include:

- **Attack surface inventory** – Provides a detailed inventory of all active hosts on the network with dozens of attributes – such as hostname, device type, services running, users logged in, etc. – extracted and maintained for each. This new feature enables security teams to gain a complete picture of the attack surface they must defend.
- **Declarations of Policy Violations™ (DoPV)** – Offers a new high-fidelity event category, similar to Declarations of Compromise™ (DoC), focused on unauthorized activity and policy violations, such as clear text passwords, outdated TLS versions, insecure cipher suites, and TOR browser usage. The detections may be tuned by the user, and users can also create custom DoPVs. This provides security and IT teams with definitive notifications of specific policy violations taking place in their organizations.
- **Improved handling of Declarations of Compromise** – Building on the powerful existing DoC capabilities, the enhancements include separate tracking of attacker assets, improved tuning, conditional behavior for automated responses, email

notifications, and inclusion in the threat hunting interfaces. These capabilities enhance defenders' ability to analyze threats and customize response automations, ultimately improving security operations efficiency and effectiveness.
- **Custom report generator with scheduler** – Delivers PDF report generation capabilities and gives users the ability to create custom reports that can leverage any system data. The system comes with several off-the-shelf options, including an "executive incident report" and a "security posture snapshot." Flexible reporting helps security operations personnel communicate with other team members and executives to improve security posture and accelerate incident response.
- **Dynamic code and algorithm updates** – Includes infrastructure for pushing new report-generating code and complex detection-as-code algorithms to the Stamus Security Platform on the fly. This capability can be used to create customer-specific custom reports, and it will soon enable the dynamic ingestion of advanced new threat detection algorithms.
- **Accelerated user experience** – With improved workflow, structured display of detection methods, and more flexible API user privileges, users have more granular access controls and enhanced understanding of event triggers for quicker event triage and rapid incident investigation.

"There are many reasons why Stamus Networks is trusted by some of the world's most targeted organizations, including government CERTs, critical infrastructure operators, central banks, insurance providers, and more," said Stamus Networks CEO Ken Gramley. "We believe our honest and transparent approach to network security helps these enterprise defenders tap into the inherent power of network traffic to cut through the clutter and focus on serious threats. Already a powerful threat detection and response tool, the updates available in U40 take the system to the next level while empowering security teams to more effectively defend their organizations, no matter how sophisticated the adversary."

Read more about U40 in today's blog article on the Stamus Networks website: https://www.stamus-networks.com/blog/ssp-u40.

Visit Stamus Networks next week in booth 2919 at Black Hat USA for a live demonstration.

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

solution that exposes serious and imminent threats to critical assets and empowers rapid response. For more information visit: stamus-networks.com.

###

Media Contact:
Jackie Gerbus
Three Rings Inc.
jgerbus@threeringsinc.com
(508) 479-2786