Stamus Networks Announces Availability of SELKS 6

The latest version of the company's open source threat hunting and IDS/IPS/NSM offering is available for download immediately

INDIANAPOLIS, USA and PARIS, FRANCE, June 16, 2020 – Stamus Networks, a fast-growing cybersecurity software company, today announced the general availability of SELKS 6 – the turnkey system based on Suricata intrusion detection/prevention (IDS/IPS) and network security monitoring (NSM) with a network threat hunting interface and graphical rule manager.

The distribution is built on the live Debian operating system with five key open source components that comprise its name – Suricata, Elasticsearch, Logstash, Kibana and Scirius Community Edition (Suricata Management and Suricata Hunting from Stamus Networks). In addition, SELKS includes components from Moloch and EveBox, which were added after the acronym was established.

"We are excited to make SELKS 6 officially available," said Peter Manev, co-founder and chief strategy officer of Stamus Networks. "This moment represents the culmination of efforts from many within the open source community, to whom we are very grateful. The new capabilities really highlight the power of threat hunting using IDS events correlated in real time with Suricata-generated metadata derived from live network traffic."

First introduced in 2014, the release of SELKS 6 represents the latest milestone for the open source system. This version includes a number of enhancements over its predecessors, including:

- **New threat hunting interface.** Improved new GUI with drill down and click-based filters based on Suricata alert data.
- **New dashboard views.** Twenty-six (26) new/upgraded Kibana dashboards and hundreds of visualizations that correlate alert events to NSM data and vice versa. Examples of the new dashboards include updates to application layer anomalies, alerts, TLS and JA3/JA3S views.
- **Updated versions of each component.** These include ELK stack (7.7.0), Suricata (6.0.0-dev), Debian (Buster), EveBox (1:0.11.1), Moloch (2.2.3), and Scirius Community Edition (3.5.0)

SELKS is a Stamus Networks contribution to the open source community and is released, at no cost, under the GNU GPLv3 license as ISO images or as source code.

In addition to its open source efforts, Stamus Networks develops and supports Scirius Security Platform™ (SSP), a commercial enterprise-scale solution. Scirius Security Platform combines real-time network traffic analysis with enhanced threat detection and an advanced analytics engine to create an entirely new class of enriched threat detection and hunting solution. This unique combination of capabilities in SSP lowers costs by eliminating the need for an additional standalone network traffic analysis (NTA) system. Visit the Stamus Networks website to learn more about Scirius Security Platform: https://www.stamus-networks.com/scirius-platform.

Kelley Misata, PhD, president and executive director of the Open Information Security Foundation (OISF) also believes SELKS 6 is an important milestone. "The OISF is thrilled to see the continued evolution of this important industry platform. We've been using SELKS exclusively in our training courses for many years because its capabilities really showcase the power of Suricata for both IDS and introductory network threat hunting," said Misata. "And these additional capabilities included in SELKS 6 will further demonstrate the value of Suricata to the community."

To download SELKS 6 and find additional information, visit the Stamus Networks open source site: https://www.stamus-networks.com/scirius-open-source.

About Stamus Networks
Stamus Networks believes cyber security professionals should spend less time pouring though noisy alerts and more time investigating true indicators of compromise (IOC). Founded by the creators of the widely deployed open source SELKS platform, Stamus Networks offers Scirius Security Platform solutions that combine real-time network traffic data with enhanced Suricata threat detection and an advanced analytics engine to create an entirely new class of enriched threat hunting solution. With Scirius, you get unprecedented visibility and meaningful insights into your organization's security posture, giving you the tools to rapidly detect and respond to incidents. For more information visit: stamus-networks.com

###

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