Stamus Networks Announces Availability of SELKS 7

The latest version of the company's open-source Suricata-based threat detection and hunting platform is available for download immediately

INDIANAPOLIS, USA and PARIS, FRANCE, April 6, 2022 – Stamus Networks, a global provider of high-performance network-based threat detection and response systems, today announced the general availability of SELKS 7 – a major upgrade to the turnkey system based on the Suricata intrusion detection/prevention (IDS/IPS) and network security monitoring (NSM) system with a built-in network threat hunting console and graphical ruleset/threat intelligence feed manager.

SELKS is now available either as a portable Docker Compose package or as turnkey installation images (ISO files). Each option includes 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 Arkime, EveBox, and Cyberchef which were added after the acronym was established.

"We are excited to make SELKS 7 officially available and in a package that makes it possible to quickly deploy on any Linux or Windows OS in either a virtual or cloud environment," said Peter Manev, co-founder, and chief strategy officer of Stamus Networks. "The improved threat hunting interface and incident response dashboards along with new Docker package, make SELKS even more accessible to folks who want to explore the power of Suricata without an investment in a commercial solution."

First introduced in 2014, the release of SELKS 7 represents the latest incarnation of the open-source system from Stamus Labs, the threat intelligence and open-source division of Stamus Networks. This version includes several enhancements over its predecessors, including:

- **Docker package.** In addition to pre-packaged Debian Linux-based ISO images, SELKS is now available as a Docker Compose package that allows SELKS to be installed on virtually any Linux or Windows system, without requiring a heavy installation process. And the docker-based architecture makes it faster and easier to deploy a new SELKS machine with specific versions of each component.
- **Fully automated PCAP replay.** Allows SELKS to easily ingest and replay PCAP directly, allowing for fast detailed analysis in training or educational applications.
- **Improved threat hunting filter sets.** Thirty-eight (38) new or updated ready-to-use threat hunting filters that help the user quickly search the Suricata alert and NSM data for shadow IT, policy violations, and suspicious activity.
- **Integrated Cyberchef.** Allows the user to apply Cyberchef encoding, decoding, and data analysis to the events, protocol transactions, and flow records created by Suricata.
- **Additional Kibana Dashboards.** Six (6) new dashboards for network visibility and hunting with new support for the following protocols: SNMP, RDP, SIP, HTTP2, RFB, GENEVE, MQTT, and DCERPC. In addition, there is a new dashboard to help those working to solve SANS Institute challenges.

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, Docker package, or as source code.

Kelley Misata, PhD, President and Executive Director of the Open Information Security Foundation (OISF) also believes SELKS 7 represents important advancements for the Suricata user community. "We are thrilled to see the continued evolution of this important Suricata showcase platform. For many years, we have used SELKS in our training courses because of its ability to showcase the power of Suricata for IDS and introductory network threat hunting based on protocol transaction and flow data," said Misata. "And we are excited for the Stamus team to bring it to the global Suricata community."

To download SELKS 7 and find additional information, visit the SELKS page on the Stamus Networks web site: https://www.stamus-networks.com/selks.

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