Stamus Networks Marks Decade of SELKS Open-Source Tool with New Edition

Free Suricata-based threat detection and hunting platform builds on open-source legacy with powerful new capabilities

INDIANAPOLIS and PARIS – June 13, 2024 – Stamus Networks, a global provider of high-performance network-based threat detection and response systems, today announced the general availability of SELKS™ 10, the latest version of its turnkey Suricata-based network intrusion detection/protection (IDS/IPS), network security monitor (NSM) and threat hunting system. The new edition, which commemorates SELKS' 10th anniversary, builds on its open-source legacy with powerful new features that enable organizations to enhance network detection and security monitoring.

Created in 2014 and available for free, SELKS is a suitable production-grade IDS and NSM solution for small-to-medium sized organizations. Because all the data available in SELKS is generated by the Suricata engine, it is widely used by network security practitioners, researchers, educators, students and hobbyists to explore what is possible with Suricata IDS/IPS/NSM and the network protocol monitoring logs and alerts it produces.

"We originally created SELKS 10 years ago as a tool to showcase the power of Suricata, and it evolved into a complete and truly useful system for smaller organizations that don't have the extensive budget and resources that enterprises do," said Peter Manev, co-founder and chief strategy officer, Stamus Networks. "Believing every organization should have the opportunity to secure their business from cyber threats, we chose to invest in SELKS to help those that can't afford a commercial solution. SELKS 10 is the latest demonstration of our continued commitment to empowering defenders with the resources they need to elevate their network monitoring and threat hunting capabilities."

Key enhancements in SELKS 10 include:

- **User interface harmonized with the Stamus Security Platform (SSP)** - The SELKS user interface has been updated to incorporate the latest capabilities of SSP, the company's commercial solution. The simplified user experience delivers consolidated threat detection and hunting and evidence views, which provides rapid insights from millions of network security events.
- **Conditional packet capture** - SELKS 10 can now capture packets (PCAP) associated with alerts. Users have access to critical network forensic data that may be used for investigation, training or threat intelligence sharing without dedicating substantial storage resources required for full-time packet capture.
- **Arkime version 5.0 features** - SELKS 10 adds the latest capabilities of Arkime bulk search, improved session detail display, unified configurations, unified authentication, JA4 support, additional multi-viewer support and offline PCAP retrieval improvements.

- **PostgreSQL database** - SELKS 10 is now using a PostgreSQL database instead of SQLite to fix known issues, augment capabilities, improve scalability, and prepare for future evolution.

SELKS is maintained by Stamus Labs, the company's open-source software and threat research team. In addition to its extensive contributions to Suricata itself, the Stamus Labs team has a rich history of open-source involvement, including introducing a set of free newly registered domain threat intelligence feeds optimized for Suricata as well as the Suricata Language Server to help streamline the rule writing process. Additionally, the team has provided a free Suricata ruleset specifically focused on detecting lateral movement in Microsoft Windows environments and published a "Security Analyst's Guide to Suricata."

Additional Resources

- To learn more about SELKS 10 features, read this blog article.
- To learn more about the 10 year history of SELKS, read last week's blog.
- To download SELKS, visit: 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. 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:
Chris Ferreira
Three Rings Inc.
cferreira@threeringsinc.com
(860) 604-0298