Stamus Networks Announces Availability of Splunk® Application

Splunk Enterprise users can now tap into the unique network security insights available from the Scirius Security Platform™ as well as open source Suricata sensors

INDIANAPOLIS, USA and PARIS, FRANCE, October 13, 2020 – Stamus Networks, a fast-growing cybersecurity software company, today announced the general availability of its application for Splunk – enabling threat hunters, incident responders and other security practitioners who use Splunk to easily gain access to the data and insights provided by Scirius Security Platform (SSP) or Suricata to more effectively do their job. The Stamus Networks App for Splunk is available immediately on Splunkbase.

"Many of our customers have been using Splunk for some time to view the basic data provided by Stamus Networks Probes through their direct Splunk connection," said Éric Leblond, co-founder and chief technology officer of Stamus Networks. "But, in order to unlock access to the advanced consolidated network capabilities of Scirius Security Platform, including host-centric insights and advanced high-fidelity threat detection, we needed to provide a custom application that adheres to Splunk's Common Information Model."

In addition to providing numerous reports and dashboards for the Scirius Security Platform, the Stamus Networks Splunk App also provides a powerful set of dashboards for users of the open source Suricata IDS/NSM. These dashboards include one specifically designed to assist Zeek users in becoming familiar with the advanced Suricata network security monitoring features such as TLS information from SMB or Kerberos activity, HTTP hosts and many other protocol transactions.

To learn more about the Stamus Networks Splunk App, visit the Stamus Networks website blog post detailing the application.

About Stamus Networks
Stamus Networks believes cyber security professionals should spend less time pouring through 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