Media Alert: Stamus Networks Releases Updated "Security Analyst's Guide to Suricata"

New version includes a chapter on DNS traffic analysis and detection

INDIANAPOLIS and PARIS – December 4, 2023 – Stamus Networks, a global provider of high-performance network-based threat detection and response systems, has published an updated version of "The Security Analyst's Guide to Suricata," a practical guide to threat hunting and detection using Suricata – the open-source intrusion detection system (IDS) and network security monitoring (NSM) engine.

The latest edition incorporates new content, featuring an important new chapter titled, "DNS Detection and Threat Hunting." The chapter provides a review of DNS-related protocols, a primer on DNS analysis using Suricata data, tips for writing rules that detect DNS activity using DNS keywords in Suricata 7, and a guide to hunting on DNS events.

Written by Stamus Networks co-founders, Éric Leblond and Peter Manev, who have both worked on Suricata development for more than 10 years, the book was first published in November 2022 and is the industry's first practical guide for unlocking the full potential of Suricata. The publication was written for security operations center (SOC) analysts and threat hunters who use Suricata to gain insights into what is taking place on their networks. The book provides vital information on entry points and in-depth analysis on the most important Suricata features, and its open-source format makes it a living book that will grow and evolve over time with ongoing input from the authors as well as contributions and feedback from the Suricata community.

PDF and eReader copies of the book can be downloaded from the Stamus Networks website, here: https://www.stamus-networks.com/suricata-4-analysts.

Additionally, hard copies of the book will be available at Black Hat Europe 2023 from December 4-7 on the show floor in stand 527.

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.