Stamus Networks Publishes "The Security Analyst's Guide to Suricata"

New book is the first practical guide for unlocking the full potential of Suricata

INDIANAPOLIS, November 7, 2022 – Stamus Networks, a global provider of high-performance network-based threat detection and response systems, today published "The Security Analyst's Guide to Suricata," a practical guide to threat detection and hunting using Suricata – the open-source intrusion detection (IDS) and network security monitoring (NSM) engine. 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.

Authors Peter Manev and Éric Leblond have been active contributors to the Suricata project for more than 10 years. And they both hold leadership positions in the organization that governs Suricata development, the Open Information Security Foundation (OISF). The pair founded Stamus Networks in 2014, a company that embeds Suricata in their commercial network detection and response (NDR) solutions to help enterprise security teams protect their organizations using their networks.

"Peter and Eric are two of the world's leading authorities on Suricata and have done an excellent job unlocking the true value of Suricata for the security analyst," said Matt Jonkman, founder and board member at OISF. "Suricata is the world's most popular open-source network security engine for threat detection and hunting. This guide gives security analysts, educators, enterprises, and even hobbyists a powerful primer to help maximize the value of Suricata in their networks."

The "Security Analyst's Guide to Suricata" is not meant to replace the user guide but was written to offer additional support for the security practitioner. The authors have taken an open-source approach to developing the content, making it a living work that will grow and evolve over time with ongoing input from the authors as well as contributions and feedback from the Suricata community. The open source content is hosted on a GitHub repository while PDF and eReader versions are available on the Stamus Networks website, here: https://www.stamus-networks.com/suricata-4-analysts.

"The idea for this book emerged after it became obvious to us that many security practitioners using Suricata either struggle to effectively use the most powerful capabilities of the tool or simply don't realize they exist," said Éric Leblond, CTO and co-founder of Stamus Networks.

“Widely known as a classic intrusion detection system (IDS), most security professionals don’t realize that Suricata can also simultaneously produce protocol and file transaction logs and flow records, and extract PCAPs and files – either independent of IDS alerts or fully-correlated with the IDS alerts. This data can provide vital information to analysts during incident investigation or threat hunting,” added Peter Manev, CSO and co-founder of Stamus Networks. “This is just one example of the information that we uncover and explain in our book,” he concluded.

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:

Taylor O’Brien
Taylor@connect2comm.com
203-733-4242