Software Engineering Institute | Carnegie Mellon University

SEI BULLETIN - SEPTEMBER 21, 2016

Traffic Analysis for Network Security: Two Approaches for Going Beyond Network Flow Data

By the close of 2016, "Annual global IP traffic will pass the zettabyte ([ZB]; 1000 exabytes [EB]) threshold and will reach 2.3 ZBs per year by 2020," according to Cisco's Visual Networking Index. The report further states that in the same time frame smartphone traffic will exceed PC traffic. While capturing and evaluating network traffic enables defenders of large-scale organizational networks to generate security alerts and identify intrusions, operators of networks with even comparatively modest size struggle with building a full, comprehensive view of network activity. To make wise security decisions, operators need to understand the mission activity on their network and the threats to that activity (referred to as network situational awareness). In this blog post, the SEI's Tim Shimeall examines two different approaches for analyzing network security using and going beyond network flow data to gain situational awareness to improve security.

Read the SEI Blog post.

SEI NEWS

- CERT Director Richard Pethia Retires
- High School Students Get Crash Course in Cyber-Kinetic Tactical Operations
- SEI Announces 2016 Watts S. Humphrey Software Process Achievement Award Winners
- SEI's Will Hayes Testifies on Use of Agile Approaches in Social Security Systems Modernization

Join Our Mailing List

Visit Our Website

STAY CONNECTED

SEI BLOG

Recent posts:

[Modeling and Simulation in Insider Threat]

[Three Strategies to Minimize the Implementation Dip in DevOps]

SEI PODCAST SERIES

Available in audio and video formats.

[Security and the Internet of Things]

[The SEI Fellow Series: Nancy Mead]

SEI EVENTS

This week's featured events:

[2016 CERT Secure Coding Symposium]

[FloCon 2017]

SEI CYBER MINUTE

SEI experts deliver weekly snapshots of our latest research on the changing world of all things cyber. This week:

[Coordinated Vulnerability Disclosure]

SEI TRAINING

Upcoming classes:

[Advanced Incident Handling]
November 14-18, 2016 (Arlington, Va.)

[Measuring What Matters: Security Metrics Workshop]
November 30-December 1, 2016 (Arlington, Va.)

SEI CAREERS

This week's featured opportunities:

[Front End Web Developer]

[Information System Security Manager]

[Cyber Security Engineer - Exercise Developer]

ABOUT THE SEI BULLETIN

The SEI Bulletin is a biweekly newsletter designed to keep you up to date on SEI news, events, research, and

other matters of interest to the SEI community. We hope you find the SEI Bulletin useful and informative.

SEND US YOUR STORY

Do you have a story abouthow an SEI technology has positively affected your team or organization? If so,the SEI would like to hear about it. Send a short summary of your success to info@sei.cmu.edu and you could be featured ina future issue of the SEI Bulletin.