Thursday, August 18, 2022
11:30 AM – 11:50 AM
Visibility Fabric Architecture for Directing Data to Central Analytics Platform

Craig Reynolds
Government Solutions
Keysight Technologies

Abstract:
To combat security threats in the operational environment, cyber operations teams and cyber protection teams rely on a wide variety of security solutions to protect networks from cyber-attacks and traffic anomalies. These tools require a variety of data sources including logs, but an ongoing critical need is the packet data itself. To enable access of critical packet data to a central platform, the program will need to deploy an intelligent high availability security visibility architecture that supports both inline and out-of-band packet processing across a distributed infrastructure.

Keysight recommends implementing the following best practices to create maximum data capture, data analysis, and network survivability during normal operations but more importantly under cyber-attack:

- Create a passive out-of-band visibility architecture to enable high speed packet capture and continuous monitoring
- Access and direct the data from physical, virtual and cloud environments
- Aggregate the signals for a unified feed to the data analysis platform, tools, and personnel
- Replication of signals allows for one-to-many distribution of the data everywhere it is required
- Traffic can be tagged to identify source origination
- Perform protocol inspection, SSL decryption, and analysis for intelligent filtering and tool optimization