Thursday, February 17, 2022
2:40 PM – 3:00 PM
Total Network Packet Analysis – The Cyber Security Force Multiplier for Zero-Day, Internal and Advanced Persistent Threat Analysis

Stephen Welles
Vice President of Federal Business Development & Government Sales
Axellio

Abstract:
Improving incident response and threat hunting is the single, most impactful means to increase your security posture. Axellio® is an innovator in threat detection and response solutions based on its highperformance PacketXpress® platform for real-time and historical network traffic analysis.

Axellio recently announced the deployment of its innovative solution by the Army's Defensive Cyber Operations for its Garrison Defensive Cyberspace Operations Platform (GDP). The current security approach of perimeter defense is insufficient for today's security risks: sophisticated threat actors with vast resources – such as nation states and global cyber-criminal organizations – that bypass conventional perimeter defense and endpoint protection with Zero-Day exploits. The resulting internal and persistent threats go undetected for months, in which cyber criminals have time to gather intelligence, stage content for exfiltration, and plant additional persistence mechanisms.

Relying on reactive, event-triggered incidents response is important, but insufficient. Investing in threat detection and response is the most impactful means to improve security posture, increasing visibility into external threat vectors, as well as internal and advance persistent threats. It reduces risk, positively impacting a variety of other security areas, including risk management, situational awareness, and data protection.

Defensive Cyber Operations need to be able to visualize the network traffic flows essential to address those threats hiding in our infrastructure, using actual network packet data for both external and internal communication. This requires packet capture and analysis capabilities that far exceed most commercially available solutions in a small enough form factor to be viable for deployment across sites.

Axellio is an innovator in high-performance, 100 Gbps no-loss network traffic capture, distribution, and analysis. Its packet capture solution provides a unique option for faster and more reliable access to richer, more contextual packet data than today's monitoring solutions. Axellio PacketXpress is an application-agnostic, open platform, combining common, off-the-shelve hardware with APIs to integrate with any existing commercial and open-source analysis solution. PacketXpress captures, stores, and forwards traffic only once - for all applications - creating a comprehensive and economical security solution for today's threats.