Tuesday, February 10

10:40 AM – 11:00 AM

Beyond Virtualization: The Real Risks Inside Today's Mobile Device Environment

Tim LeMaster

VP Federal Systems Engineering

Lookout

Abstract:

The DoD relies on Virtual Mobile Infrastructure (VMI) solutions like Hypori to ensure Zero-Data-at-Rest. But this strategy is based on a lethal fallacy: VMI does not protect the device itself. In an era of nation-state-level threats, a pixel stream is not a perimeter.

This is a failure point that hostile adversaries are exploiting daily. Sophisticated, zero-click spyware—like Pegasus—bypasses the virtual container entirely, compromising the underlying physical device's OS. Once the endpoint is compromised, the attacker can silently mirror the screen to steal credentials, exfiltrate native OS data (SMS, call logs, and geolocation), and nullify the VMI's security assumptions. The warfighter's device, network, and communications are wide open.

This session cuts through the buzzword-driven hype to reveal the non-negotiable DoD security mandates (including the Apple iOS/iPadOS STIG) that demand Defense-in-Depth. We will demonstrate why a single-point solution—VMI—is insufficient. The only True Zero Trust architecture for mission assurance requires a layered approach:

MDM + VMI + The Mandatory Mobile Threat Defense (MTD) Layer.

Learn how the critical MTD layer provides continuous, deep device monitoring to detect advanced threats before they can compromise the virtual session, closing the unacceptable security gap that virtualization leaves wide open. Don't trust isolation; demand active, device-level protection.