Thursday, June 27, 2024

11:30 AM - 11:50 AM

Enhancing DoD's AI Threat Intelligence with Comprehensive Datasets

Tim LeMaster

Vice President, Worldwide Systems Engineering

Lookout

Abstract:

The Department of Defense (DoD) has reportedly experienced a staggering 12,000 cyber incidents since 2015. This relentless assault from cybercriminals and nation-state actors on classified data and DoD systems is not just a security concern but a direct threat to the critical infrastructure and the safety of U.S. citizens.

Artificial Intelligence (AI) is a powerful tool for combating these ongoing threats, enabling insights to enhance threat detection and response capabilities. However, DoD must build future-ready AI programs based on quality datasets that account for all data types, including mobile data.

In today's digital era, many government employees use mobile devices during work, whether agency-issued or employee-owned. With over half of personal mobile devices targeted by phishing attacks in 2022, mobile data is a threat vector that must be considered when training AI models and increasing analysts' ability to defend critical DoD systems.

Over the last decade, Lookout has collected the world's most extensive mobile threat dataset, comprising telemetry from more than 210 million devices and 280 million apps and insights from more than 410 million URLs and 17,500 SaaS apps. In this session, Tim LeMaster, Lookout's Vice President, Worldwide Systems Engineering, will:

- Discuss best data practices for strengthening AI models and improving their ability to identify and correlate cyberattacks.
- Highlight how mobile threat intel can strengthen DoD's data pipeline and enable a better understanding of the latest criminal tactics threatening national security
- Examine Lookout's mobile dataset to gain insights into the new tactics being leveraged by criminals