Wednesday, June 26, 2024

11:30 AM - 11:50 AM

Intersection of AI and Security

Gina Scinta

Deputy Chief Technology Officer

Thales Trusted Cyber Technologies

Abstract:

Artificial intelligence (AI) is rapidly transforming our world, from the way we work to the way we interact with machines. But with this immense power comes immense responsibility. As AI becomes more sophisticated, so too do the potential security risks.

This session will discuss the critical issues at the intersection of AI and security. The speaker will explore:

• Countering malicious use of AI systems by actors with ill intentions, such as criminals, terrorists, or hostile states.

• Adversarial attacks on AI, such as attempts to fool or manipulate AI systems by exploiting their vulnerabilities or limitations.

• Protection of the massive amounts of data used by AI systems to learn and improve their performance.

• Using AI to enhance cybersecurity, such as preventing cyberattacks, optimizing security processes, and improving security resilience.