Tuesday, October 22, 2024

2:00 pm - 2:20 pm

Best Practices for Implementing Quantum-Resistant Security

Gina Scinta

Deputy CTO

Thales TCT

Abstract:

Quantum computing's potential computational power will render today's widely-deployed encryption algorithms obsolete. Both the National Security Memorandum on Promoting US Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems and Quantum Computing Cybersecurity Preparedness Act stress the need to update IT infrastructure today to combat the quantum threat. Both policies emphasize the use of crypto-agile solutions to diminish transition time and enable seamless updates to new cryptographic standards.

In August 2024, NIST, academia, and industry in reached the milestone of releasing the first set of Post Quantum Cryptography (PQC) standards. This milestone is a result of many years of research, development, testing, and collaboration. Now, federal agencies are tasked with moving to the next phase of getting standards-compliant, interoperable solutions deployed to combat the looming quantum threat.

Session attendees will learn about the best practices that federal agencies should follow when transitioning to quantum-resistant security including how to:

• Utilize crypto inventory tools to learn where and how encryption is currently deployed within an agency's infrastructure

• Prioritize existing infrastructure for a migration to post-quantum cryptography

• Deploy crypto-agile solutions for PKI, Data-at-Rest and in-Transit, and Identity and Access Management

• Apply a Cryptographic Bill of Materials (CBOM)