



Future-Proofing Your Data

A Simplified Guide to Quantum-Safe Encryption

International Cyber Expo, London

October 2025



Julian Fay

Chief Technology Officer

Senetas

www.senetas.com

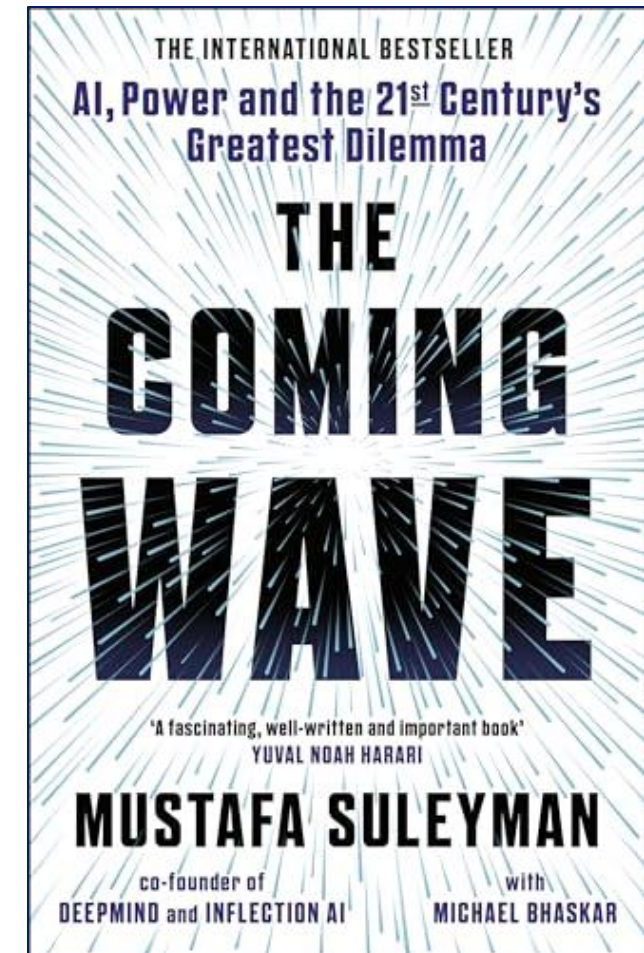
"We are on the cusp of the most important Transformation of our lives".

"Essentially, the entire post-war security and economic order is facing unprecedented strain".

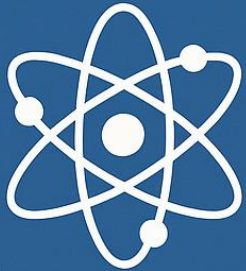
AI = Engineering Intelligence

Synthetic Bio = Engineering Life

Quantum = Engineering Reality



UK National Quantum Strategy 2024–2034



Leading
the future
by 2033



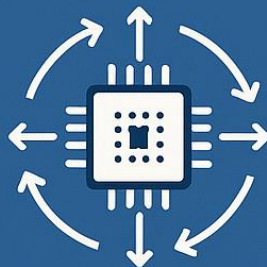
£2,5B + £1B **10 years**



World-leading
research
& skills



Magnet for
business,
investors & talent



Accelerate
adoption across
economy & security



Shape regulation
& safeguard
UK capabilities

QUANTUM AND CYBER SECURITY OPPORTUNITIES AND RISKS

Opportunities

(Enhancing Security & Defence)



Strengthen national security, resilience & competitiveness



Quantum communications
→ secure, high-bandwidth, covert links



Quaxtum sensing/timing →
next-gen Position, Navigation
& Timing (PNT)



Advanced machine learning,
data fusion & modelling
for defence

Threats

(Cryptography at Risk)



Quantum computers
will break today's public-key
cryptography



First-mover nations gain
decisive security
advantages

Cryptographically Relevant Quantum Computer

A Quantum Computer big enough to perform Quantum Cryptanalysis

Dictionary

Definitions from [Oxford Languages](#) · [Learn more](#)

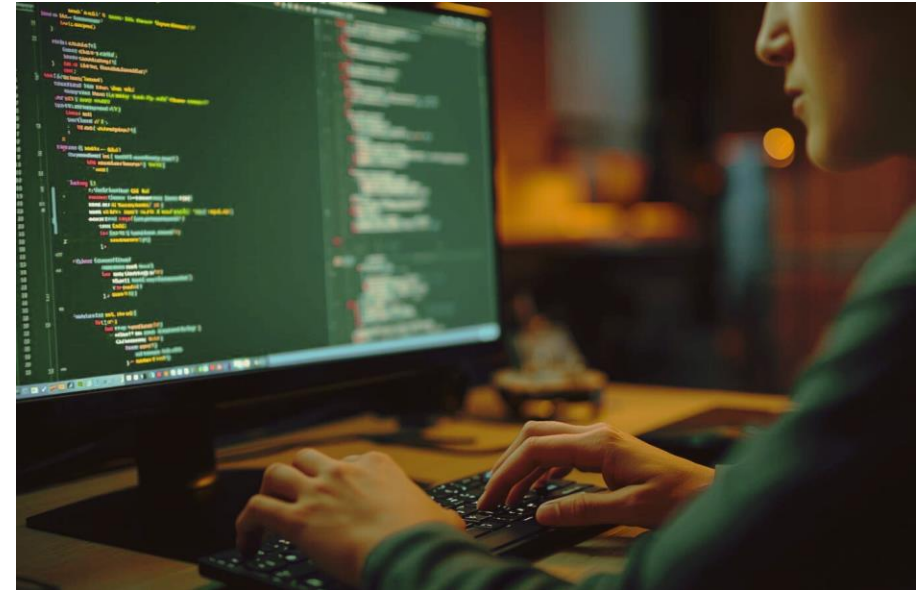


cryptanalysis

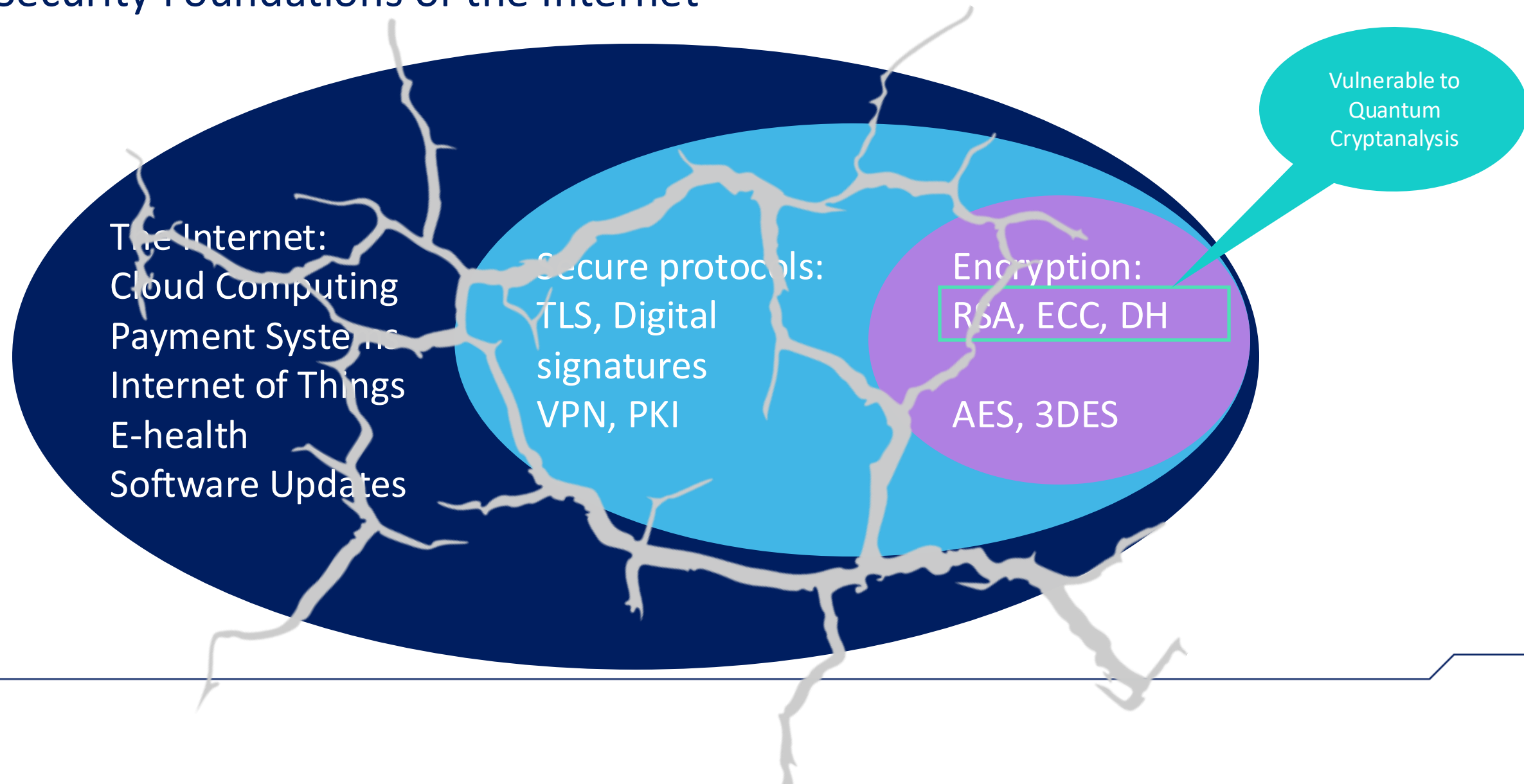
/ˌkrɪptəˈnælɪsɪs/

noun

the art or process of deciphering coded messages without being told the key.



Security Foundations of the Internet



Areas of High Risk



Forge Signatures

- Impersonate entities
- Load malicious OS patches
- Create fraudulent financial transactions
- Redirect funds



Human in the Middle Networks

- Access secure systems
- Compromise military command and control
- Disrupt critical infrastructure
- Interfere with elections

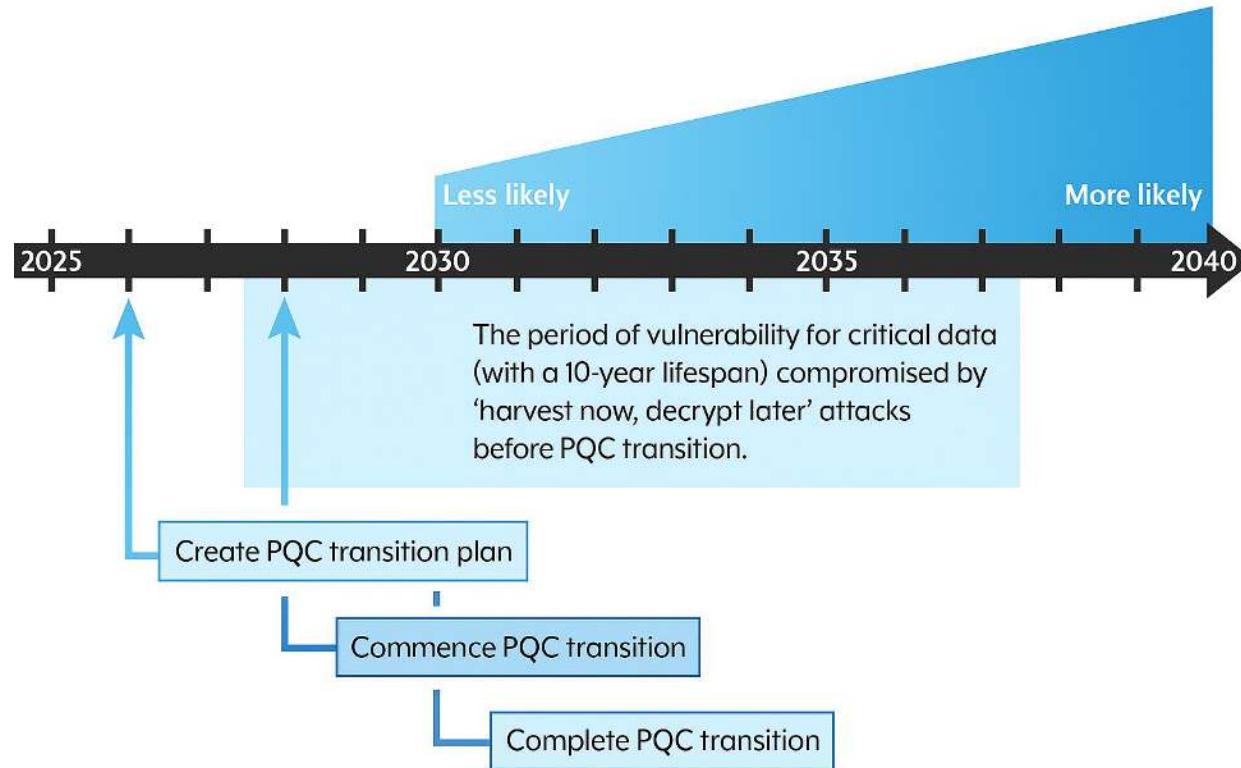


Decipher Historical Confidential Data

- Intercept classified comms
- Expose government secrets
- Perform corporate espionage
- Access personal information

When should we worry?

Estimated likelihood of achieving CRQC*



*CRQC – Cryptographically Relevant Quantum Computer

Harvest Now, Decrypt Later attack



Example: Harvest Now, Decrypt Later attack

NEWS Last update: November 7, 2024

'Salt Typhoon': How Chinese hackers spied on US security officials



IMAGO / VCG

EXCLUSIVE

Chinese hackers gained access to huge trove of Americans' cell records

Investigators aren't sure how much data Salt Typhoon might have taken, and are still struggling to evict the elite Chinese hacking crew from companies' networks.



The possible theft of cell records pertaining to millions of Americans has become one of the leading concerns for investigators as they struggle to evict Salt Typhoon from some of the nation's leading phone companies. | George Frey/AFP/Getty Images

The "Harvest Now, Decrypt Later" Strategy

Perhaps most concerning is how Salt Typhoon's operations align with China's broader "harvest now, decrypt later" strategy. This approach involves collecting massive amounts of encrypted data today, anticipating future quantum computing capabilities that could decrypt this information. As quantum computing advances, previously secure encryption methods may become vulnerable, potentially exposing years of stored sensitive data.

New Cryptography for the Quantum Age

NIST Released First Three Post-Quantum Encryption Standards in 2024

ML-KEM

- Formerly CRYSTALS-KYBER
- FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism

ML-DSA

- Formerly CRYSTALS-Dilithium
- FIPS 204 Module-Lattice-Based Digital Signature Standard

SLH-DSA

- Formerly SPHINCS+
- FIPS 205 Stateless Hash-Based Digital Signature Standard

FN-DSA

- Formerly FALCON
- Designed for digital signatures
- Slated for its own draft FIPS in 2025

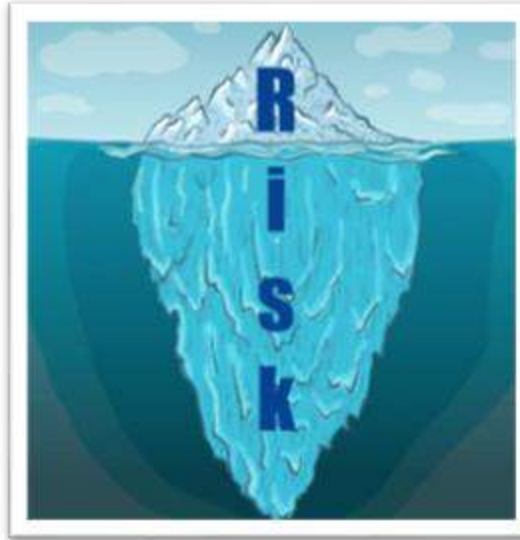


Standardization
Forthcoming

The PQC Migration Challenge



Scale

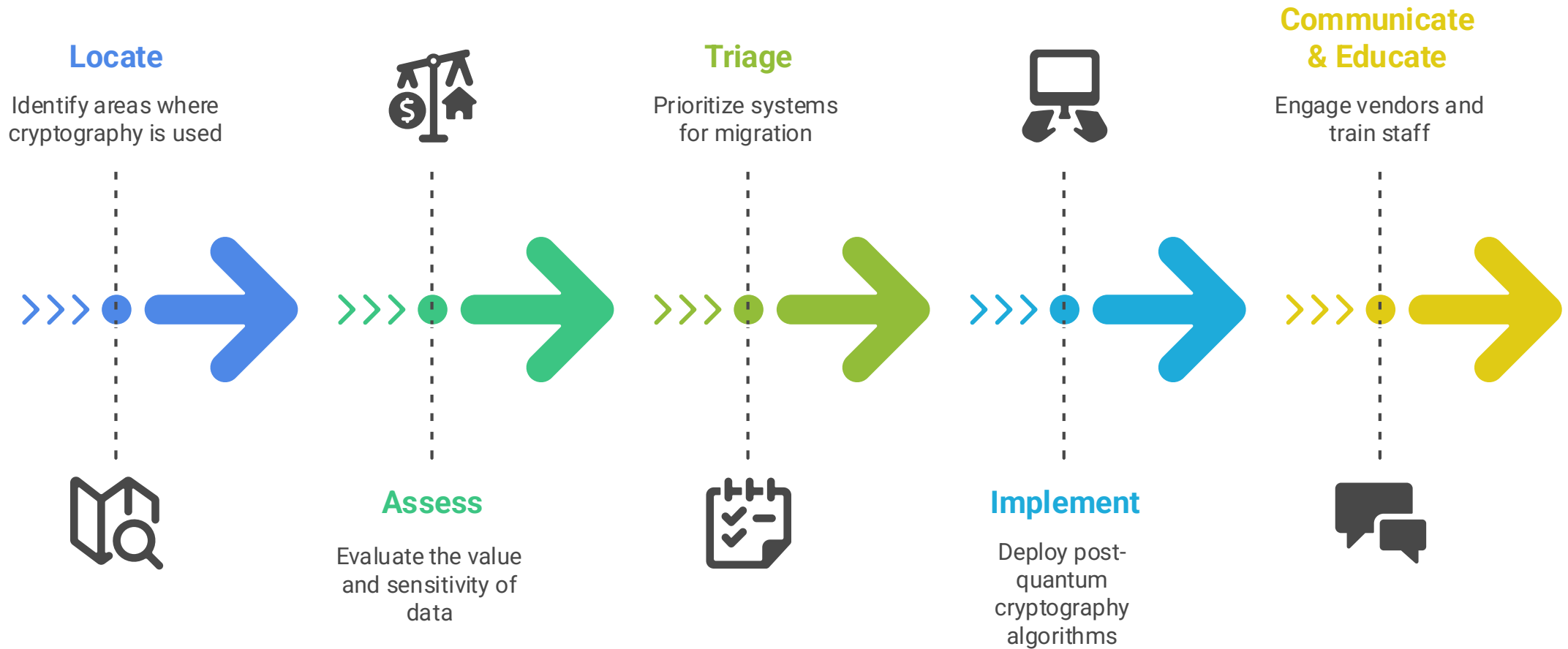


Visibility

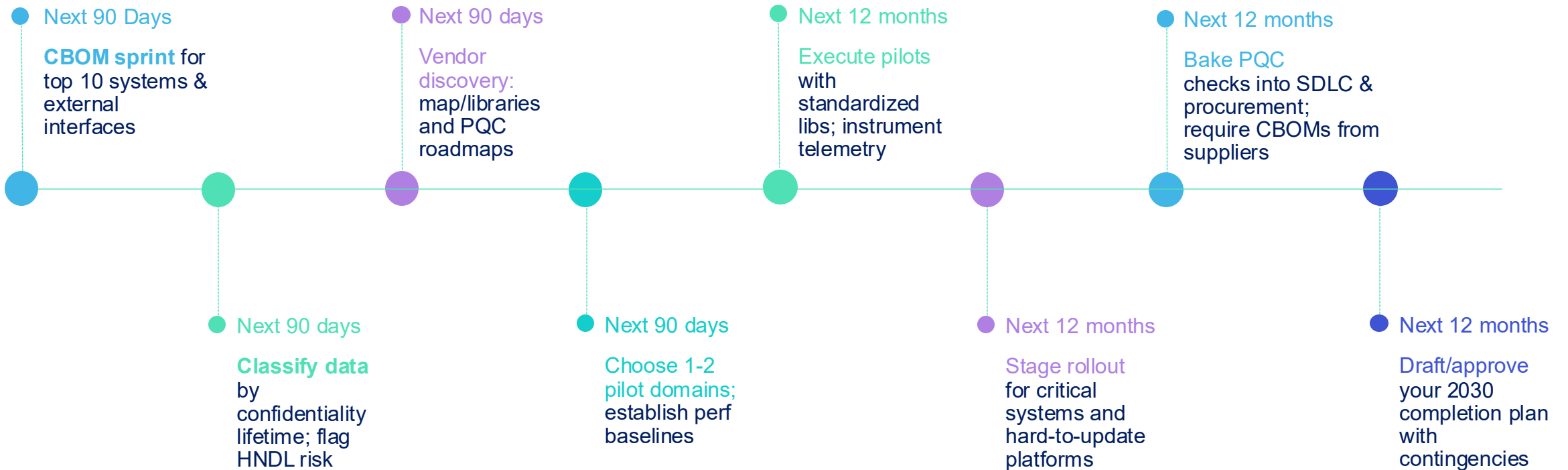


Data lifetimes

Lattice Framework: Cryptography Migration Process



Strategic Action Plan for System Enhancement



Commercially available: Quantum-safe High Speed Encryptors (HSE)



Senetas CN7107



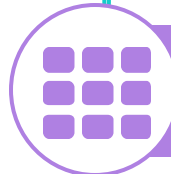
Quantum Resistant Algorithms

- Support NIST PQC/QRA



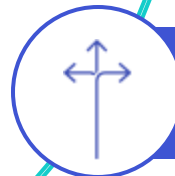
Quantum Key Distribution

- HSE has supported QKD for over a decade



QRNG

- QRNG is integrated into the HSE solution*



Crypto Agility

- HSE supports Post Quantum Cryptography (PQC) with a crypto-agile, FPGA-based architecture

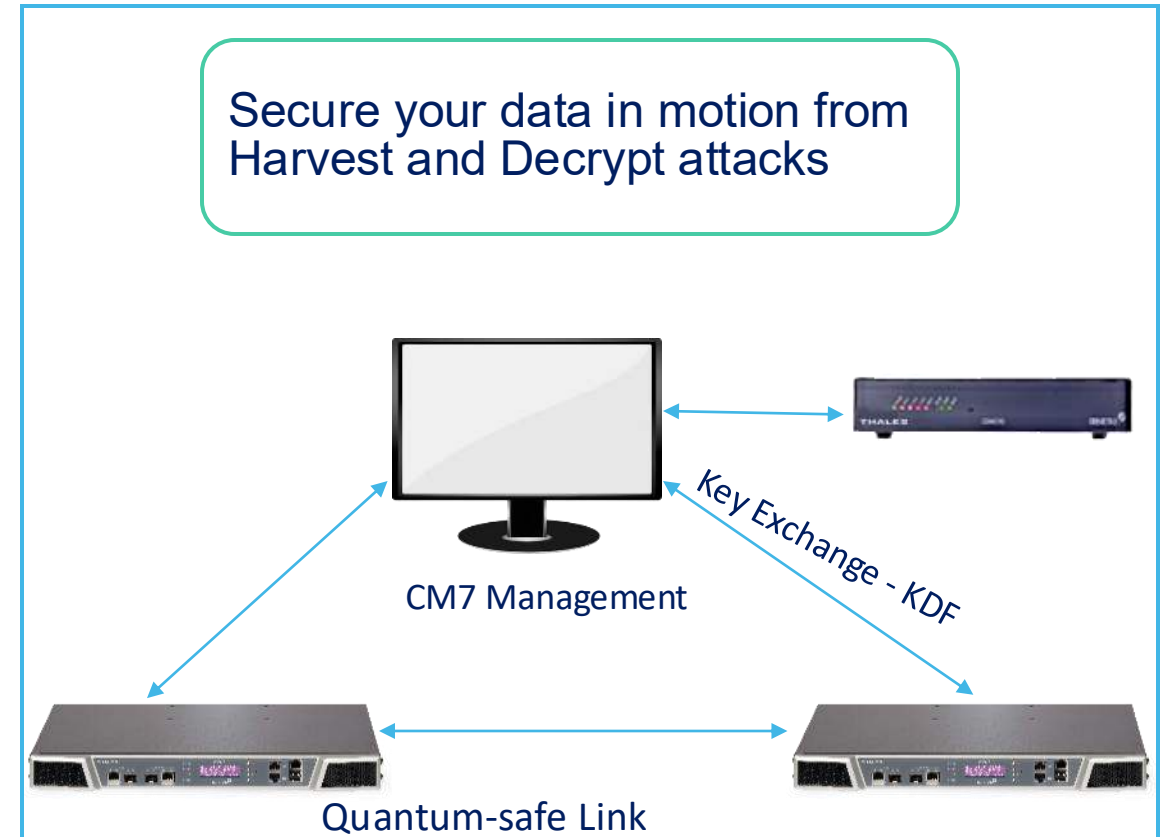
*Model specific



Thales PQC HSE Starter Kit

Easily set up your Quantum-safe test environment with:

- NIST Post-Quantum algorithms implemented
- Out of band key management, NIST approved KDF method
- Quantum Key Distribution via ETSI eQKD v14.01
- Optional QRNG or External Entropy Source (BYOE)
- Minimize disruption to your business by leveraging the Thales partner ecosystem as you prepare for [PQC](#).



Company Overview

Proven Track Record

Over 25 years securing sensitive data across 60+ countries.

Global Reach, Local Expertise

Deployed in partnership with Thales, a global leader in advanced technologies.

Defense & Industrial-Grade Solutions

Australian-designed and manufactured encryption and secure file sharing platforms.

Future-Ready Performance

Solutions use quantum-resistant, future-ready encryption that adapts as new cybersecurity standards emerge.

Cross-Sector Trust

Trusted by government, defense, financial services, critical infrastructure, and professional services.

Independently Certified

Technology certified by global security authorities and standards, including Common Criteria, FIPS, DoDIN APL and NATO.





Thank you

senetas.com