Cyberdefense

Post-Quantum Transformation

Building resilience for the quantum era - before it's too late.

The encryption protecting your organisation today will be broken by quantum computers. The threat isn't future — attackers are already harvesting your encrypted data now, ready to decrypt it the moment quantum capabilities catch up. This is "Harvest Now, Decrypt Later." And most organisations are nowhere near ready.

$3tn
Global financial assets at risk from quantum computing (Citibank, 2026)

5%
enterprises have started to implement PQC algorithms (DigiCert, 2025)

2029
ENISA deadline for completing PQC transition

Why choose this offer?

- **8 years of PQC expertise**
  Orange Applied Cryptography Group has contributed to NIST and ISO PQC standardisation since 2017. Our consultants helped shape the standards your migration will follow.
- **Business-first approach**
  We quantify your quantum risk in financial and regulatory terms before recommending any technical action.
- **End-to-end coverage**
  One partner from strategic roadmap through discovery to migration execution and continuous assurance.
- **Crypto-agility by design**
  Flexibility built into your governance and architecture from day one.
- **Proven tooling**
  Backed by our partners' cryptographic discovery solution for asset visibility at scale.

What's the engagement about?

PQC migration is not a **simple algorithm swap**. Cryptography is embedded across your entire organisation — in TLS connections, VPNs, certificates, APIs, authentication systems and payment flows. Most organisations have **no clear inventory** of where it lives or which assets carry the highest risk

Our engagement begins with assessing your **business, regulatory environment, and cryptographic posture** to evaluate **quantum risk** and create a **strategic roadmap**. We then establish governance, provide training, and conduct discovery to map and prioritize your cryptographic assets. Based on these insights, we develop a **phased migration plan** aligned with risk and market maturity, delivering it iteratively from discovery to execution, with ongoing support to maintain and adapt your **cryptographic resilience**.

Find out more about our PQC Migration offer online:
https://orangecyberdefense.com/global/postquantumcryptography

How it works

Our engagement follows a progressive three-phase journey, designed to meet your organisation where it is and scale at your pace.

Phase 1 — Advisory & Strategic Roadmap

The right entry point for organisations beginning their PQC journey. We assess your quantum risk and prepare a business case taking into consideration your buisness priorities, data longevity, regulatory exposure and migration readiness to deliver a prioritised transformation roadmap.

Phase 2 — Discovery, Classification & Inventory

Our OCD consultants leverage specialised partner tooling to identify and catalogue cryptographic assets across your environment - networks endpoints, applications, cloud, source code and third parties, using a use-case and phased discovery approach.

Phase 3 — Migration & Continuous Assurance

Phased deployment of hybrid and quantum-safe algorithms across prioritised assets. We establish crypto-agility policies, supply-chain requirements and continuous monitoring to keep your organisation quantum-safe as standards evolve.

What's in the deliverables?

- Quantum risk and impact assessment with cost-to-delay scenarios
- Full cryptographic inventory by system and environment
- Regulatory gap analysis across ENISA, ANSSI, NIST and ECB frameworks
- Prioritised PQC migration roadmap with ROI assessment
- Governance framework and cryptographic policie
- Trainings for internal IT teams
- Technology and vendor recommendations

Why Orange Cyberdefense?

As Europe's leading cybersecurity company, Orange Applied Cryptography Group has been involved in Post-Quantum Cryptography for 8 years — contributing to NIST and ISO PQC standardisation, publishing world-class research, and playing an active role in our customers' projects. We are also a QUALIOPI-certified training centre, offering dedicated PQC programmes to equip your teams for the transition ahead.

Our engagement's are backed by our trusted partners' specialised cryptographic discovery tooling and delivered by 3,000+ cybersecurity experts worldwide — combining deep cryptographic knowledge with local execution. With 50,000+ customers globally, we help organisations stay secure and compliant, today and in a post-quantum world.