

CyberSeQ™

Quantum-Resilient Cybersecurity for Critical Infrastructure

CyberSeQ™ is a deep-tech cybersecurity company based in Germany and the UK. We enable governments, telecoms, and regulated industries to migrate from vulnerable classical encryption (RSA, ECC) to post-quantum cryptography (PQC). Our platform, PostQ, automates this transformation—making systems crypto-agile, compliant, and future-proof.

As quantum computers evolve, existing cryptographic standards will no longer suffice. CyberSeQ ensures critical systems remain secure and verifiable, even in a post-quantum world.

PostQ Platform

Automated Migration to Quantum-Safe Encryption

PostQ is a modular platform that detects, upgrades, and manages cryptographic components across enterprise systems.

Core Functions:

- Crypto Discovery – Maps all cryptographic assets via our CADI engine
- AI-Powered Refactoring – Replaces outdated algorithms with quantum-safe ones
- Credential Issuance – Issues digital certificates, tokens, and identities in hybrid (classical + PQC) formats
- Protocol Upgrade – Adds PQC support to VPNs, TLS, SSH, and cloud endpoints
- Compliance Tools – Aligns with NIST, ETSI, BSI, and FIPS standards

Integrated with AWS, Azure, GitHub, and enterprise platforms, PostQ delivers secure deployment without disrupting existing systems.

Q-SIEM & Infralytics

Quantum-Aware Monitoring & Infrastructure Intelligence

CyberSeQ's advanced modules go beyond migration:

- Q-SIEM – A cryptography-aware monitoring system for detecting threats, weak configurations, and migration gaps
- Infralytics – A compliance engine visualizing cryptographic posture, entropy usage, and identity flows across infrastructure considering NIS2, CRA, DORA, ISO27K and more

Our Ecosystem

We collaborate with hardware partners (e.g., Quantum Brilliance) and contribute to European PQC standards and testing environments. Current deployments include telecom, financial, and defense pilots in critical sectors.