One PQC journey for IT and OT

Secure, Assure and SOAR bring infrastructure context, application evidence and a governed response together, so each migration decision has evidence and an owner, and your team can check again after each change.

The transition problem

Post-quantum cryptography (PQC) migration is a program of evidence, ownership and controlled change. Leaders need to know which services matter, where cryptography is used, what can change safely, and how the team will check each change afterwards. QASO helps with the evidence; your team plans and makes the changes.

Secure

Records the systems, services and exposure its collector can see on networks you authorize, and the key exchange a service selects in a TLS 1.3 test connection. Not proof the network is complete, and not a full cryptography inventory.
Leaves: a record of what was seen, and the questions that still need evidence.

Assure

Reviews application source code and its dependencies, cites the exact line of each finding, and lists the cryptography the code calls. Engineering candidate: not yet approved for your source code, for installation at your site, or for production use.
Leaves: source-linked findings and a list of cryptography calls, by file and line.

SOAR

Investigates operational signals, can rehearse a proposed change on a rehearsal copy (a simulation), and drafts a response approved according to its risk class.
Leaves: a drafted response and its approval or policy log. Your team makes the change.

01 / Scope

Choose critical services and how long their information must stay protected.

02 / Map

Connect systems, services, repositories and owners, with evidence for each link.

03 / Plan

Your team designs the cryptographic and operational change.

04 / Change and check

Your team makes the change; re-run Secure or Assure to see the new state.

System context

What Secure saw, and what remains unseen.

Source evidence

Where cryptography is called in application code.

Decision record

Who approved the proposed response, by risk class.

Your change record

What your team changed, and what remains classical.

Evidence › Accountable owner › Decision › Your change › Check again

Discover where cryptography is used

The first milestone is a bounded view of critical systems, applications, trust relationships and information lifetimes, with every relationship either supported by evidence or visibly unresolved.

Start with the information that must remain trustworthy

Prioritize by information lifetime, operational consequence, migration duration and external dependency. Long-lived data and difficult-to-change operational-technology (OT) systems may need action early. OT protocols are safety-critical: confirm how plant equipment is collected before a pilot.

Secure: system context

Records reachable systems, services and known weaknesses, and the key exchange a TLS 1.3 test connection selects. It does not read certificates or test older TLS versions, SSH or tunnels.

Assure: source evidence

Locates cryptographic calls in source and dependencies, keeping the exact code, the scan scope and how far each finding was checked. Engineering candidate: not yet approved for your source code, for installation at your site, or for production use.

Your records

Add supplier, platform, certificate and device statements with their source, date and owner. They stay your records; QASO does not verify them.

Build a migration register leaders can use

Service and owner

Critical service, business unit, accountable owner and business consequence.

Information lifetime

How long confidentiality, authenticity or integrity must last.

Cryptographic role

Key establishment, signature, certificate, protocol or stored-data dependency.

Evidence and freshness

Observed, source-linked, supplier-declared or inferred, with a date and scope.

Migration path

Target standard, compatibility boundary, testing and recovery plan (your team's).

Decision state

Investigate, plan, change, check again, accept temporarily, or retire.

Boundary to keep

Secure planning examples do not establish your cryptographic use. Source, customer, supplier and platform evidence keep separate origins until the link between a system, a service and a repository is confirmed.

Move from findings to a planned change

Application and infrastructure evidence meet at the service boundary: what must change, who owns it, how operations stay safe, and how your team checks the result.

Turn evidence into migration work

Assure links cryptographic findings to exact source, dependencies and, where one is assigned, an engineering owner. Secure supplies system and service context once the link to a repository is confirmed. SOAR records the proposed response and how it was approved. QASO does not perform or prove a migration.

Prepare the change

Name the cryptographic role, target standard, compatibility window, supplier dependency, data that must stay readable, and the recovery condition.

Change through your process

Your team uses its own source, certificate, protocol, firmware or configuration process, with approvals, exceptions and temporary measures kept explicit.

Check again

Re-run Secure or Assure after the change to see the new state, and record the classical dependencies that remain.

IT migration

Coordinate code, libraries, certificates, identity systems and deployment pipelines. Use staged compatibility and a new Secure or Assure run after deployment.

OT migration

Account for supplier firmware, maintenance windows, safety constraints, long service lives and limited rollback. Keep operational continuity and compensating controls in your own records.

Your team's change record

Before

The implementation and dependency baseline your team recorded.

Change

The approved change, its target and your execution record.

After

A new Secure or Assure run showing what it can now see.

Remaining

Exceptions, classical dependencies and the next review.

Recorded baseline › Owned design › Approved change › Checked again

Govern the transition with evidence

A staged program keeps operational control while standards, suppliers and systems change, and gives leadership a defensible basis to fund, sequence and check the next move.

Keep operations safe during a long transition

SOAR can bring supported evidence into an investigation, rehearse a proposed change on a rehearsal copy, and prepare a response approved according to its risk class (automatic with a log for the lowest class; named people above that). Temporary containment may reduce a specific exposure; it does not replace PQC migration or make previously exposed data quantum-safe.

Govern by business unit

Keep scope, permissions, evidence and exceptions separate. Map shared services and dependencies explicitly.

Measure progress

Report critical-service coverage, freshness, unresolved dependencies, accepted exceptions and the changes your team has made and checked again.

Decide in stages

Expand, narrow, pause or stop based on reproducibility, operating effort, control readiness and residual risk.

Cross-product views

Each product can stand alone. Joined views need supported imports, a common review window and explicit system, service and repository identifiers; similar names do not prove a relationship.

Urgent operating posture

Narrow the scope to the critical service and the highest-consequence exposure. Your team prepares a reversible compensating control, keeps the approval and recovery plan, and checks again afterwards.

Provenance

Origin, time basis and collection or source boundary.

Authority

Approval by risk class, with named people above the lowest class; each human approval expires.

Recovery

A rollback step in every SOAR proposal; your team's recovery plan for the change itself.

Check again

A new Secure or Assure run after your team's change.

Known › Owned › Changed by your team › Checked again