ETSI/IQC Quantum Safe Cryptography Conference 2025

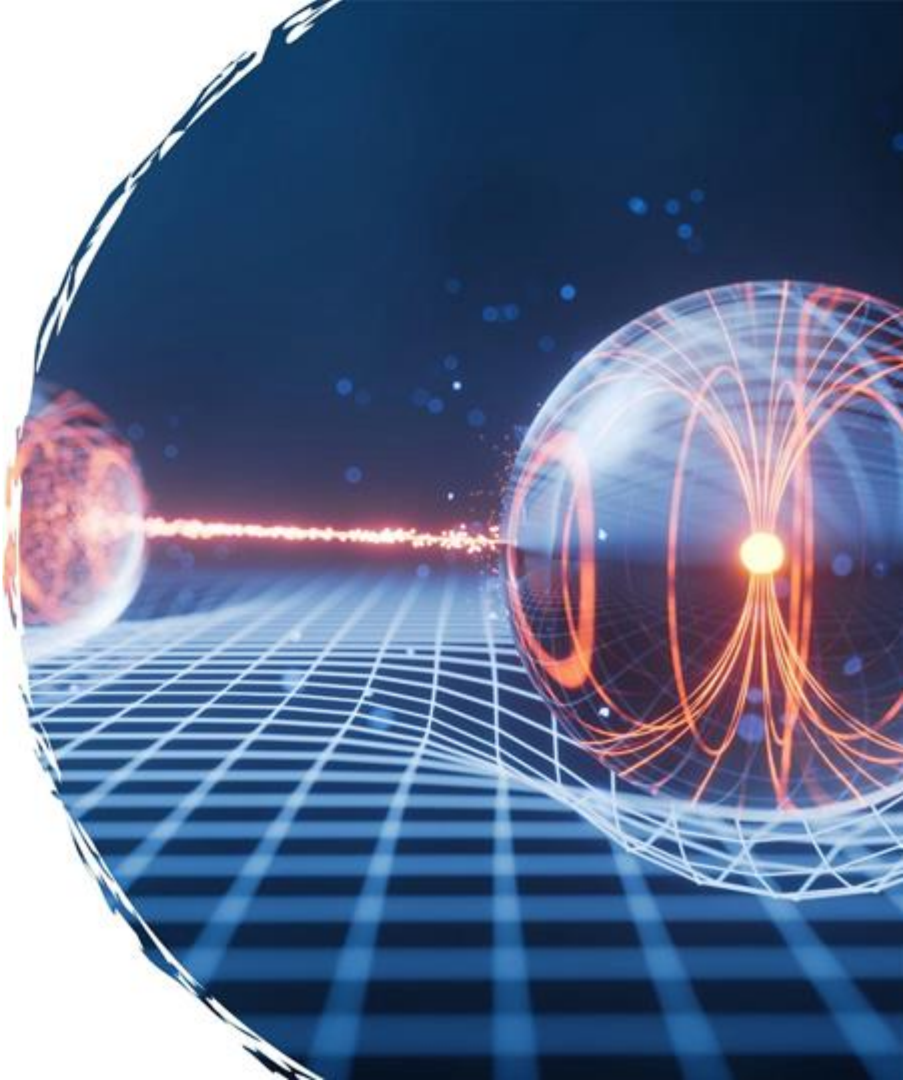
Lessons learned from the field: Cryptographic Insight from the Modern Enterprise

James Howe

Staff Research Scientist & ETSI QSC Vice-Chair

SANDBOXAQ

05/06/2025



Presentation outline

1 **The PQC Challenge**
Understanding enterprise complexities.

2 **A New Approach**
Integrated discovery and management, utilizing existing infrastructure.

3 **Real-World Insights**
Practical lessons learned.

4 **Achieving Agility**
Outcomes and the path forward.

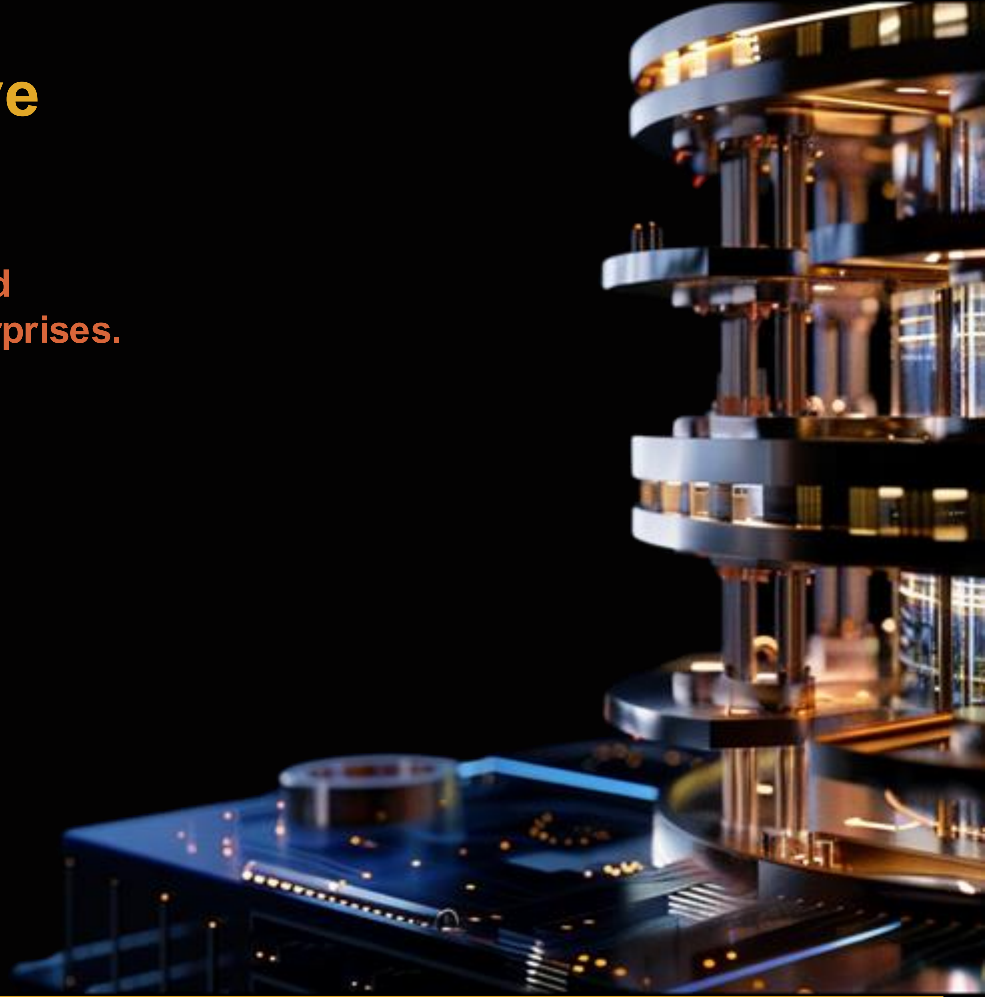
The PQC Migration Imperative

The quantum threat and the urgent need for PQC.

PQC migration

A complex, multi-faceted challenge for large enterprises.

- Vast, distributed IT environments
- Numerous legacy systems and cryptography
- Fragmented software ecosystem
- Disparate and diverse hardware



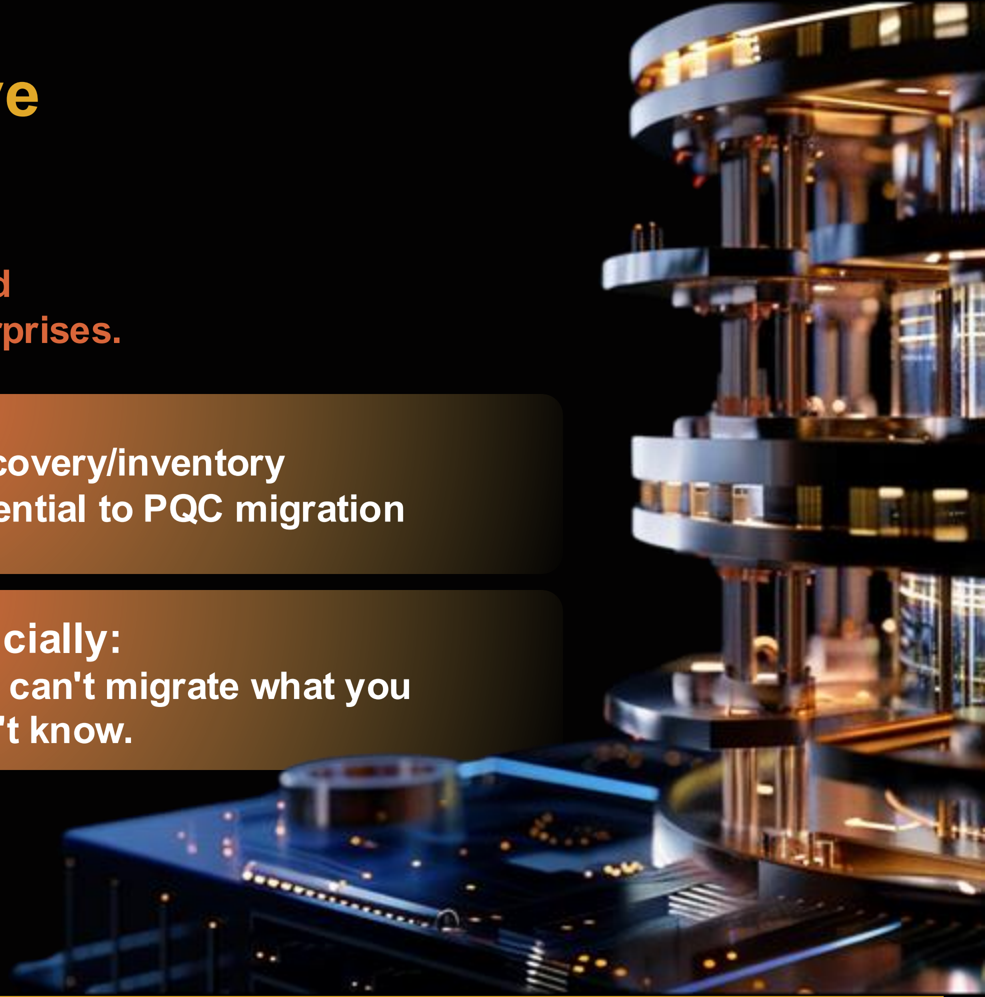
The PQC Migration Imperative

The quantum threat and the urgent need for PQC.

PQC migration

A complex, multi-faceted challenge for large enterprises.

- Vast, distributed IT environments
- Numerous legacy systems and cryptography
- Fragmented software ecosystem
- Disparate and diverse hardware



Discovery/inventory essential to PQC migration

Crucially:
You can't migrate what you don't know.

The Enterprise Landscape

Complexity & Fatigue

Complex IT Footprint

Vast, distributed, multi-country environments with diverse hardware and legacy systems.

Visibility Gaps

Hard to get holistic view of crypto assets & NHIs.

Tool Fatigue Burden

Enterprises are overwhelmed by siloed tools; no resources for new, non-integrated solutions.

Alert Fatigue Overload

Security teams are drowning in alerts, missing critical issues, burnout.

Cryptographic Discovery

Current Hurdles at Scale

- Traditional reliance on custom agents, scanners, and sensors.
- These offer detailed insights and 360-degree coverage.
- Enterprise-scale deployment/management presents scalability and operational issues.
- Numerous deployments demand substantial resources for installation, maintenance, and ongoing management.
- Navigating this landscape requires strategic planning for full visibility and clear PQC remediation.

Deepening Insight

Practical Integrations with Key Tools

Holistic approach
Bridges data silos for unparalleled cryptographic visibility.

Creates overall data landscape map, leveraging CMDBs and other tool insights.

Qualys.

Import certificate, secrets & TLS configs to analyze potential crypto. vulnerabilities & misconfigurations

CROWDSTRIKE

Orchestrates filesystem scanning to enable seamless scanning of remote hosts.

servicenow

Ingest certificate/asset data from its CMDB capabilities for centralized management & enhanced security posture

Ingest data to enhance key management and security monitoring.

paloalto NETWORKS

Ingest and analyze TLS handshake data from Next-Generation Firewall log files.

CBOM
Cryptography Bill of Materials

Upload/analyze CBOMs for comprehensive insight.

Lessons from the Field

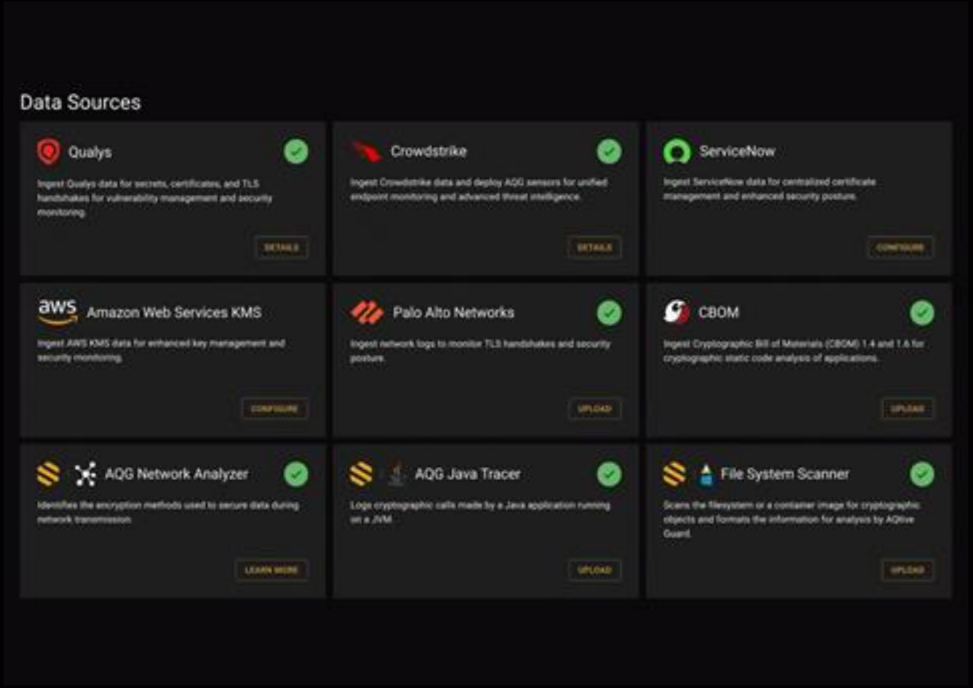
Customer-Driven Innovation

Customer feedback revealed key pain points

- High operational overhead managing numerous, siloed security agents.
- Drove the development of 3rd party ingestion for faster time-to-value, optimizing sensor deployment.
- Reduced alert fatigue via unique alerts.
- Enabled flexible asset profiling.

This feedback loop was critical for refining the solution.

Moved from "what we thought was needed" to **"what customers actually need."**



Data Sources

Qualys

Ingest Qualys data for secrets, certificates, and TLS handshakes for vulnerability management and security monitoring.

Crowdstrike

Ingest Crowdstrike data and deploy AQG sensors for unified endpoint monitoring and advanced threat intelligence.

ServiceNow

Ingest ServiceNow data for centralized certificate management and enhanced security posture.

Amazon Web Services KMS

Ingest AWS KMS data for enhanced key management and security monitoring.

Palo Alto Networks

Ingest network logs to monitor TLS handshakes and security posture.

CBOM

Ingest Cryptographic Bill of Materials (CBOM) 1.4 and 1.6 for cryptographic static code analysis of applications.

AQG Network Analyzer

Identifies the encryption methods used to secure data during network transmission.

AQG Java Tracer

Logs cryptographic calls made by a Java application running on a JVM.

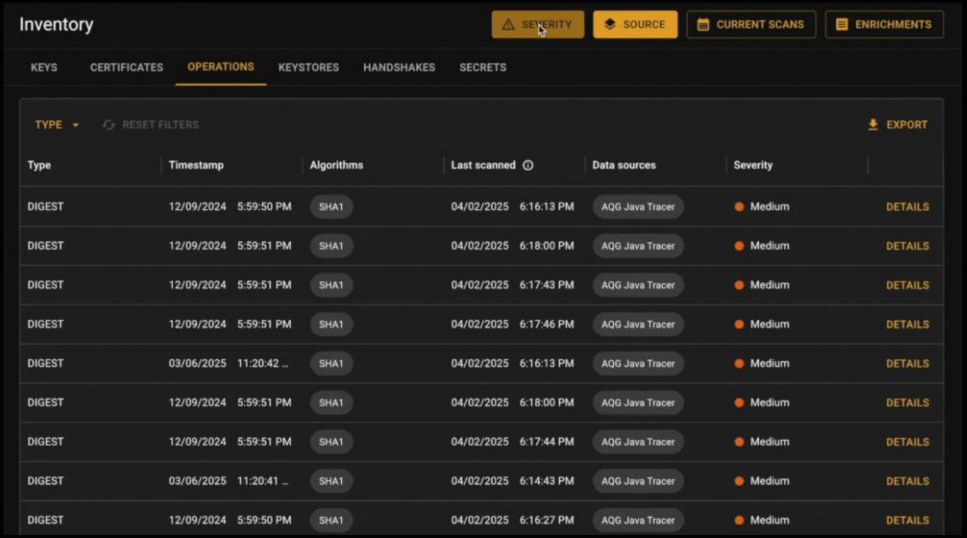
File System Scanner

Scans the filesystem or a container image for cryptographic objects and formats the information for analysis by AQtive Guard.

Enhancing Insight

Advanced Intelligence & Actionable Filtering

- Unifies deep data from existing 3rd-party tools & first-party sensors.
- Yields actionable, meaningful data and rich context on assets and identities.
- Advanced correlation links assets to endpoints, apps, and owners for key context.
- Intelligent filtering reduces noise, delivering advanced insights with broader context.
- Deep enrichments provide rich context: '*Is this crypto mine? Do I care?*'
- Provided Knowledge graph transforms data into clear, prioritized PQC steps.



Type	Timestamp	Algorithms	Last scanned	Data sources	Severity	
DIGEST	12/09/2024 5:59:50 PM	SHA1	04/02/2025 6:16:13 PM	AQG Java Tracer	● Medium	DETAILS
DIGEST	12/09/2024 5:59:51 PM	SHA1	04/02/2025 6:18:00 PM	AQG Java Tracer	● Medium	DETAILS
DIGEST	12/09/2024 5:59:51 PM	SHA1	04/02/2025 6:17:43 PM	AQG Java Tracer	● Medium	DETAILS
DIGEST	12/09/2024 5:59:51 PM	SHA1	04/02/2025 6:17:46 PM	AQG Java Tracer	● Medium	DETAILS
DIGEST	03/06/2025 11:20:42 ...	SHA1	04/02/2025 6:16:13 PM	AQG Java Tracer	● Medium	DETAILS
DIGEST	12/09/2024 5:59:51 PM	SHA1	04/02/2025 6:18:00 PM	AQG Java Tracer	● Medium	DETAILS
DIGEST	12/09/2024 5:59:51 PM	SHA1	04/02/2025 6:17:44 PM	AQG Java Tracer	● Medium	DETAILS
DIGEST	03/06/2025 11:20:41 ...	SHA1	04/02/2025 6:14:43 PM	AQG Java Tracer	● Medium	DETAILS
DIGEST	12/09/2024 5:59:50 PM	SHA1	04/02/2025 6:16:27 PM	AQG Java Tracer	● Medium	DETAILS

Realizing Cryptographic Agility

Outcomes & Impact

Reduces Tool Fatigue
Minimizes new deployments; scales efficiently for large orgs.

Mitigates Alert Overload
Delivers prioritized, actionable insights; focuses teams on critical exposures.

Clear Remediation Path
Guides large orgs where to start PQC migration, even with vast crypto assets.

Simplifies PQC Transition
Streamlines move to PQC.

Enhances Security Posture
Improves crypto agility and organizational risk readiness.

Key Takeaways & Future Outlook

Smart Discovery is Key: PQC migration success relies on intelligent discovery, not just more tools.

Integrate for Efficiency: Leverage existing enterprise data and infrastructure for scale.

Actionable Insights: Prioritize context and understanding over raw data volume.

Agile Cryptography: Drive future readiness via intelligent system utilization.

Call to Action: Engage with modern crypto and machine identity approaches.

SANDBOXAQ™

Thanks for listening!

Any questions?