Press Release

FOR IMMEDIATE RELEASE

QuDef launches SQOUT®, the first Quantum Threat Intelligence Platform for QKD and Quantum Communication Systems

The platform addresses a critical gap as Quantum Key Distribution (QKD) moves from research labs into national infrastructure, satellite networks, and enterprise deployments — where every system assessed to date has shown previously unknown or unmitigated vulnerabilities.

Delft, 1st of June 2026 — QuDef today announced the commercial availability of **SQOUT®**, the first dedicated Quantum Threat Intelligence and Security Assessment platform for Quantum Key Distribution (QKD) and other quantum communication systems. SQOUT gives CISOs, risk managers, red and blue teams, QKD vendors, integrators, and certification bodies a single operational tool to model, assess, and defend the quantum communication systems now being deployed across Europe and beyond.

QKD protocols such as BB84, BBM92, CV-QKD, and MDI-QKD are theoretically secure under their underlying assumptions. In practice, however, real-world implementations are exposed to side-channel attacks, detector blinding, Trojan-horse attacks, assumption violations, and implementation gaps that traditional cybersecurity tooling is not designed to detect.

In 100% of the QKD systems QuDef has assessed to date, SQOUT has identified vulnerabilities that were either unknown to the operator or not yet mitigated.

"Quantum communication has moved out of the lab. It is now being deployed in initiatives like EuroQCI, on quantum satellites such as Eagle-1, and inside enterprise networks handling some of the most sensitive data in the world," said Bob Dirks, CEO at QuDef. *"The technology is ready. The threats are real. What was missing was an operational way for the people responsible for these systems, e.g.CISOs, regulators, integrators, and red teams, to actually treat quantum security as a security and risk-management process rather than a research topic. That is the gap SQOUT closes."*

What SQOUT does
SQOUT provides a unified platform that allows security and engineering teams to:

- Understand the evolving quantum threat landscape, with continuously updated intelligence on attacks, vulnerabilities, and countermeasures relevant to quantum communication systems.
- Model QKD and other quantum communication system architectures, including their optical, electronic, and protocol-level components.
- Identify exploitable weaknesses and implementation risks, including known side channels and emerging attack vectors specific to quantum hardware.
- Translate complex attack paths into prioritised, actionable mitigations that map to the operational reality of CISOs, certification bodies, and national authorities.

The platform is built around four core modules — QBuilder, QAnalyser, QKill, and a roadmap extending toward QNetwork, QAssessment and QCompliance — covering everything from architectural modelling to attack scenarios and forthcoming compliance workflows.

Deployment options
To meet the requirements of both commercial and sovereign customers, SQOUT is available in multiple deployment models:

- **Software-as-a-Service (SaaS)** via QuDef's secure web-based infrastructure.
- **On-premises Virtual Machine deployment** for classified and sovereign environments.
- **SQOUT as a Service**, in which QuDef experts deliver assessment and audit engagements directly on behalf of the customer.

A **free open-access edition** is also available at **sqout.qudef.com**, offering a public preview of SQOUT's core capabilities. Organisations seeking to evaluate the full platform and its applications in depth can request a trial licence by contacting QuDef directly.

Who it is for
SQOUT is built for any organisation deploying, integrating, certifying, or defending quantum communication systems, including:

- CISOs and security teams operating or procuring QKD infrastructure
- Risk and compliance managers assessing quantum-related exposure
- Red and blue teams extending their scope to quantum systems
- QKD vendors and integrators seeking to validate and harden their products
- National authorities and certification bodies establishing assurance frameworks for quantum communication

About QuDef
QuDef is a quantum security company dedicated to making the quantum communication infrastructure of the future verifiably secure in practice — not only in theory. Through SQOUT and its associated services, QuDef helps governments, critical infrastructure operators, and quantum technology vendors close the gap between theoretical quantum security and operational reality.

QuDef – Securing the Quantum Frontier.

Media contact: dr. Bob Dirks, CEO QuDef, contact@qudef.com
Note to editors: A demo of SQOUT, technical briefings, and interviews with QuDef's quantum security experts are available on request.