INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-11 14:57 UTC

QIZ Security Raises $17M Seed Round to Accelerate Post-Quantum Cryptography Transition

SECURITY ANALYSIS | **CRITICAL**

SCC Item ID	SCC-STY-2026-0347
Type	Security Analysis
Severity	CRITICAL
Affected Products	Critical infrastructure (general), organizations relying on current asymmetric encryption standards (RSA, ECC, Diffie-Hellman)
Published	2026-07-10
Discovery Source	Gemini

Executive Summary

QIZ Security's $17 million seed round reflects growing enterprise concern about post-quantum cryptography migration, driven by the harvest now, decrypt later threat model in which adversaries collect today's encrypted data for future decryption once cryptographically-relevant quantum computers emerge. NIST finalized three post-quantum cryptography standards in August 2024 (FIPS 203, 204, and 205), establishing a migration baseline that CISA, NSA, and NIST have jointly urged critical infrastructure operators to act on immediately. For CISOs and boards, this funding round is a market signal: the PQC transition window is open, the standards exist, and organizations that defer inventory and planning now face compounding remediation costs and potential regulatory exposure as timelines tighten.

Technical Analysis

The harvest now, decrypt later (HNDL) threat model does not require a quantum computer today. Adversaries, particularly nation-state actors with long operational horizons, are assessed to be intercepting and archiving encrypted network traffic now, with the intent to decrypt it once cryptographically-relevant quantum computers (CRQCs) become viable. The threat specifically targets asymmetric encryption schemes, including RSA, elliptic curve cryptography (ECC), and Diffie-Hellman key exchange, which underpin the confidentiality of the majority of enterprise and critical infrastructure communications.

The NIST PQC standardization process, completed in August 2024, established three actionable standards: FIPS 203 (ML-KEM, a key encapsulation mechanism based on the CRYSTALS-Kyber algorithm), FIPS 204 (ML-DSA, a digital signature algorithm based on CRYSTALS-Dilithium), and FIPS 205 (SLH-DSA, a stateless

hash-based signature scheme). These standards provide the cryptographic primitives needed to begin migration, but the migration process itself, involving cryptographic inventory, protocol assessment, vendor dependency mapping, and phased implementation, is operationally complex and time-intensive, typically spanning multiple years for large enterprises and critical infrastructure operators.

CISA, NSA, and NIST have issued joint guidance urging organizations to treat this as a planning-now problem rather than a future problem. The 2029 horizon cited for potential CRQC viability represents an aggressive estimate within a range of government and academic projections; the agencies' consistent message is that timeline uncertainty does not reduce urgency, because the inventory and transition work required spans years. The QIZ Security funding round reflects a growing commercial recognition that most large organizations lack the internal tooling and expertise to execute this transition without specialized assistance. Critical infrastructure sectors, including energy, finance, healthcare, and government, face the highest exposure given the sensitivity and longevity of the data they protect and the long operational lifecycles of their underlying systems.

Action Checklist

1. Step 1: Assess cryptographic exposure, inventory all systems, protocols, and data flows that rely on RSA, ECC, or Diffie-Hellman key exchange, prioritizing those protecting long-lived or high-sensitivity data (aligns with CIS 2.1: Establish and Maintain a Software Inventory, and CIS 3.2: Establish and Maintain a Data Inventory)
2. Step 2: Review NIST PQC standards, obtain and evaluate FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) for applicability to your current cryptographic implementations; consult CISA and NSA joint PQC guidance for critical infrastructure-specific migration sequencing
3. Step 3: Update threat model, incorporate the HNDL threat vector into your threat register; assess which archived or in-transit data streams are most valuable to long-horizon adversaries and prioritize their protection accordingly
4. Step 4: Develop a phased migration roadmap, establish a documented cryptographic transition plan with milestones; query vendors on PQC migration timelines and FIPS 203/204/205 support commitments for hardware, software, and network infrastructure dependencies (aligns with CIS 7.1: Establish and Maintain a Vulnerability Management Process)
5. Step 5: Communicate findings to leadership, brief the board and C-suite on HNDL exposure specific to your organization's data sensitivity and operational sector, framing the risk in terms of regulatory, reputational, and operational continuity implications rather than purely technical terms
6. Step 6: Monitor regulatory and standards developments, track NIST, CISA, and NSA publications for additional PQC guidance, and watch for sector-specific regulatory mandates that may impose migration timelines on critical infrastructure operators

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to CISO and legal counsel if threat intelligence indicates that encrypted data transmitted by your organization has been observed in adversary collection operations (e.g., via ISAC reporting or government notification), if a sector-specific regulator issues a PQC migration mandate with a deadline under 12 months, or if cryptographic inventory reveals RSA/ECC protection on data with regulatory breach-notification obligations (PII, PHI, CUI) and no crypto-agility capability exists to insert ML-KEM or ML-DSA without a multi-year re-architecture.
Recovery Notes	Post-migration verification must confirm that ML-KEM (FIPS 203) key encapsulation and ML-DSA or SLH-DSA (FIPS 204/205) signatures are actively negotiated in production TLS, VPN, and PKI workflows — validate via `openssl s_client` cipher suite output and certificate signature algorithm inspection, not merely configuration file review. Monitor for hybrid-mode fallback events where endpoints negotiate classical RSA/ECC rather than PQC algorithms, as these indicate incomplete migration coverage and continued HNDL exposure; log algorithm negotiation outcomes at the TLS termination point for at least 90 days post-cutover. Retain pre-migration encrypted traffic archives under legal hold if there is any possibility that adversary collection has already occurred, as these may become evidence in future regulatory or legal proceedings.
Forensic Artifacts	TLS handshake negotiation logs from load balancers, reverse proxies (e.g., nginx access logs with `$ssl_cipher` and `$ssl_protocol` variables), and VPN concentrators — these establish which cipher suites were in use during the HNDL collection window and which data streams were protected only by RSA/ECDH | PKI certificate inventory exports (e.g., output of `certbot certificates`, HSM audit logs, or CA issuance records) documenting RSA/ECC key sizes and validity periods — these define the temporal scope of cryptographic exposure for data signed or encrypted under now-vulnerable keys | Network flow records (NetFlow/IPFIX or pcap archives) from internet-facing ingress/egress points covering the past 3–5 years — in an HNDL scenario these represent the adversary's potential collection corpus of encrypted sessions that may be decrypted retroactively once a cryptographically-relevant quantum computer is available | SSH algorithm negotiation logs (e.g., OpenSSH `LogLevel VERBOSE` output capturing `kex: algorithm` lines) and IKEv2 phase-1 proposal logs from VPN gateways showing DH group selection — these identify encrypted administrative and site-to-site channels exposed to harvest-now collection | Application-layer encryption configuration files and key management system audit trails (e.g., HashiCorp Vault audit logs, AWS KMS CloudTrail events for GenerateDataKey/Decrypt calls) — these document which data-at-rest encryption operations used RSA/ECC wrapping keys and therefore which stored data blobs are subject to future quantum decryption if key material was exposed

Per-Action IR Details

Step 1: Assess cryptographic exposure — inventory all systems, protocols, and data flows that rely on RSA, ECC, or Diffie-Hellman key exchange, prioritizing those protecting long-lived or high-sensitivity data (aligns with CIS 2.1: Establish and Maintain a Software Inventory, and CIS 3.2: Establish and Maintain a Data Inventory)

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing visibility into the cryptographic attack surface before quantum-capable adversaries can exploit harvested ciphertext

Controls: CIS 2.1 (Establish and Maintain a Software Inventory), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: For a 2-person team without enterprise discovery tooling: run `openssl s_client -connect :443 2>/dev/null | grep 'Server public key'` across perimeter hosts to fingerprint RSA/ECC key sizes; use `nmap --script ssl-enum-ciphers -p 443,8443,636,993,995` to enumerate cipher suites advertising DHE/ECDHE; inventory TLS certificates via `certbot certificates` or `find /etc/ssl -name '*.pem' -exec openssl x509 -noout -text -in {} \; | grep 'Public

Key Algorithm'`; document results in a spreadsheet mapping asset → algorithm → data sensitivity tier → estimated data retention period.

Evidence: This step does not alter live state and therefore does not require volatile capture prerequisites. However, document baseline cryptographic posture now as a timestamped audit artifact: export current TLS certificate inventory, cipher suite configurations, VPN/SSH algorithm negotiation logs (e.g., OpenSSH `AuthorizedKeysFile` entries, IKE phase-1 logs showing DH group selection), and any PKI CA signing algorithm configurations — these establish the pre-migration baseline against which future compliance is measured.

Step 2: Review NIST PQC standards — obtain and evaluate FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) for applicability to your current cryptographic implementations; consult CISA and NSA joint PQC guidance for critical infrastructure-specific migration sequencing

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: acquiring authoritative guidance and technical standards that define the migration target state, analogous to establishing detection signatures before a known campaign goes active

Controls: NIST SI-5 (Security Alerts, Advisories, And Directives)

Compensating: For a 2-person team: bookmark and schedule monthly review of https://csrc.nist.gov/projects/post-quantum-cryptography and CISA's PQC initiative page; download the FIPS 203/204/205 final standards PDFs directly from NIST CSRC and map each algorithm to your current use cases (key encapsulation → ML-KEM replacing RSA/ECDH; digital signatures → ML-DSA or SLH-DSA replacing RSA-PSS/ECDSA); use the NSA CNSA 2.0 algorithm table as a sequencing reference for national security system operators.

Evidence: This is a standards-review step and does not alter live system state; no volatile capture is required. Retain a timestamped record of which standards versions were reviewed and the gap analysis conclusions — this documentation supports future audit and regulatory inquiries from sector-specific regulators (e.g., NERC CIP for energy, HIPAA for health) regarding demonstrated due diligence in PQC awareness.

Step 3: Update threat model — incorporate the HNDL threat vector into your threat register; assess which archived or in-transit data streams are most valuable to long-horizon adversaries and prioritize their protection accordingly

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: integrating the harvest-now-decrypt-later threat model into organizational risk posture so that detection and response planning accounts for retrospective decryption of previously captured encrypted traffic

Controls: NIST IR-8 (Incident Response Plan), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: For a 2-person team: use a structured threat register spreadsheet with columns for threat actor category (nation-state with long-horizon collection mandates), attack vector (passive interception of RSA/ECC-encrypted TLS/VPN traffic), affected data tier (classified, PII, IP, OT control plane), estimated sensitivity window (how many years the data retains value), and current cryptographic exposure; prioritize data streams with sensitivity windows exceeding 5–10 years — the commonly cited horizon for cryptographically-relevant quantum computers — using CISA's PQC migration prioritization guidance for critical infrastructure sectors.

Evidence: This step does not alter live state and requires no volatile capture. As a forensic-forward practice, identify and preserve packet capture samples of high-sensitivity encrypted data flows (e.g., archived PCAP files from network taps or NetFlow records) that may already have been collected by adversaries — these samples define the 'already harvested' exposure boundary and should be referenced in the threat register to quantify HNDL blast radius.

Step 4: Develop a phased migration roadmap — establish a documented cryptographic transition plan with milestones; engage vendors on PQC roadmap commitments for hardware, software, and network infrastructure dependencies (aligns with CIS 7.1: Establish and Maintain a Vulnerability Management Process)

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: building the remediation capability and vendor coordination structure required to execute cryptographic migration before quantum-capable adversaries can operationalize harvested ciphertext

Controls: NIST SI-2 (Flaw Remediation), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For a 2-person team: structure the roadmap in three phases — (1) crypto-agility hardening (enable algorithm negotiation flexibility in TLS 1.3 configurations so FIPS 203/204/205 can be inserted without full re-architecture); (2) hybrid mode deployment (run ML-KEM alongside ECDH in parallel, as supported by OpenSSL 3.2+ and liboqs); (3) classical algorithm deprecation — with explicit milestone dates tied to NIST's published deprecation schedule (RSA/ECC deprecated by 2030 per NIST IR 8547 draft); track vendor PQC readiness using public roadmap disclosures from hardware HSM vendors (Thales, Entrust), VPN vendors, and certificate authorities.

Evidence: This step does not alter live cryptographic configurations and does not require volatile capture as a prerequisite. Document the current-state algorithm inventory (from Step 1) as the migration baseline artifact — any future audit will require evidence that pre-migration cryptographic posture was formally recorded before transition activities began.

Step 5: Communicate findings to leadership — brief the board and C-suite on HNDL exposure specific to your organization's data sensitivity and operational sector, framing the risk in terms of regulatory, reputational, and operational continuity implications rather than purely technical terms

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: translating technical cryptographic risk findings into executive-level risk communication and organizational policy action, analogous to lessons-learned reporting that drives governance changes

Controls: NIST IR-6 (Incident Reporting)

Compensating: For a 2-person team without a dedicated GRC function: prepare a one-page risk brief quantifying HNDL exposure in business terms — for example, estimate the volume of encrypted data (in TB or transaction count) transmitted over RSA/ECC channels in the past 5–10 years that adversaries could have passively collected, identify the regulatory frameworks that mandate cryptographic controls for your sector (NERC CIP-005 for energy, HIPAA §164.312(a)(2)(iv) for healthcare, CMMC Level 2 for defense contractors), and cite CISA/NSA joint advisories as the authoritative source establishing the threat's credibility; use the NIST NCCoE PQC migration project as a reference for peer organization adoption timelines.

Evidence: This is a governance communication step with no live system state changes; no volatile capture is required. Retain the briefing materials, attendee records, and any board resolutions or executive decisions as governance artifacts — these demonstrate organizational awareness and due diligence in the event of future regulatory inquiry or post-incident review following a confirmed HNDL-related data exposure.

Step 6: Monitor regulatory and standards developments — track NIST, CISA, and NSA publications for additional PQC guidance, and watch for sector-specific regulatory mandates that may impose migration timelines on critical infrastructure operators

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: establishing continuous intelligence collection on the evolving PQC regulatory landscape to ensure migration roadmap milestones remain aligned with mandatory compliance deadlines as they are finalized

Controls: NIST SI-5 (Security Alerts, Advisories, And Directives), NIST AU-6 (Audit Record Review, Analysis, And Reporting)

Compensating: For a 2-person team: configure RSS feeds or email subscriptions for NIST CSRC (csrc.nist.gov), CISA advisories (cisa.gov/news-events/cybersecurity-advisories), and NSA Cybersecurity Advisories; set a quarterly calendar reminder to review NIST IR 8547 (Transition to Post-Quantum Cryptography Standards) for deprecation schedule updates and check sector-specific regulatory bodies (NERC, HHS, FCC, FFIEC) for PQC mandate publications; maintain a regulatory watch log with issue date, source, applicability to your sector, and any imposed deadline.

Evidence: This is a continuous monitoring and governance step with no live state changes; no volatile capture is required. Maintain a dated regulatory watch log as an audit artifact demonstrating ongoing due diligence — in the event that a sector regulator imposes a retroactive compliance deadline, this log establishes that the organization was actively tracking the requirement and can substantiate good-faith migration progress.

Detection Guidance

Post-quantum cryptography transition planning does not generate traditional IOC-based detection, but organizations can audit their exposure and detect readiness gaps through the following approaches:

Cryptographic inventory audit: Identify all certificate authorities, TLS configurations, VPN protocols, code-signing pipelines, and key management systems using RSA, ECC, or Diffie-Hellman. Tools such as network traffic analyzers and TLS inspection proxies can enumerate negotiated cipher suites across the environment.

Data classification review: Assess which archived or in-flight data streams carry long-term sensitive value (intellectual property, regulated personal data, national security-adjacent information). These are the primary HNDL targets.

Vendor cryptographic roadmap assessment: Query critical vendors and supply chain partners for their PQC migration timelines and FIPS 203/204/205 support commitments. Gaps here represent third-party risk.

Policy gap audit: Review existing cryptographic policy against NIST SP 800-53 SI-7 (Software, Firmware, and Information Integrity) to confirm integrity verification mechanisms will remain valid post-migration. Audit key management and rotation procedures against D3-CRO (Credential Rotation) and D3-CH (Credential Hardening) to ensure these processes can accommodate new algorithm families.

Log review: Check SIEM and network monitoring logs for anomalous bulk data exfiltration patterns that could indicate HNDL collection activity in progress, even if decryption is not yet possible for the adversary (aligns with NIST AU-6: Audit Record Review, Analysis, and Reporting, and NIST SI-4: System Monitoring).

Framework Mappings

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **SC-13** — Cryptographic Protection

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission Security

Sources

Source	URL	Tier
Critical Infrastructure Security and Resilience	https://www.cisa.gov/topics/critical-infrastructure-security-and-re...	T1
Critical infrastructure and cybersecurity	https://energy.ec.europa.eu/topics/energy-security/critical-infrast...	T1
Vulnerability-analysis-in .pdf	https://securityanddefence.pl/pdf-108665-40437?filename=Vulnerabili...	T3
The weakness in global critical infrastructure cybersecurity	https://www.weforum.org/stories/cybersecurity/dangerous-blindspot-i...	T3

Generated 2026-07-11 14:57 UTC by TJS Security Command Center