QUANTUM FOUNDRY

Penetration Testing with Quantum Security Readiness

The Core Proposition

A penetration test finds what's exploitable now. A cryptographic vulnerability assessment finds what will be exploitable when quantum computing matures.

Neither is optional anymore, and running them separately means you never see how they connect.

Quantum Foundry works across classical networking and quantum-safe infrastructure, which means the findings come with a clear path to remediation, not just a list of what's broken.

Quantum Foundry

CYSTEL

SECTION 1

What Is the Quantum Foundry Pen Test

The Quantum Foundry pen test is a single offensive security engagement that shows what an attacker can exploit in your environment today and what cryptographic posture will become exploitable as quantum computing matures. It combines deep manual penetration testing with a quantum security readiness assessment under **one statement of work, one delivery team, and one correlated risk register**, so security leaders can see present-day exposure and future-state cryptographic risk in one place.

Instead of treating quantum risk as a separate strategy exercise, the engagement ties it directly to active attack paths, business-critical assets, and the controls your organization will need to defend over the next several years. That makes it easier to prioritize remediation, brief leadership, and build a defensible plan before harvest-now-decrypt-later attacks become a practical reality.

Built For Regulated Enterprises

Financial services, energy and utilities, healthcare systems, defense supply chain, large pharma, and critical telecommunications all share the same challenge: they protect long-lived sensitive data that may remain valuable for years, or even decades. These sectors also operate under named regulatory and contractual obligations such as OCC, NERC CIP, HIPAA, CMMC, PCI DSS 4.0, and SEC 10-K disclosure expectations. That combination makes them prime targets for harvest-now-decrypt-later campaigns, where attackers capture encrypted data today and wait for quantum advances to break it later.

For these organizations, the question is not whether quantum risk matters, but how soon they need evidence, prioritization, and a remediation path tied to the systems most exposed to both current offensive techniques and future cryptographic failure.

Strategic Importance

The CISO, CRO, or Head of Compliance is already accountable for cryptographic risk, already fielding questions from auditors and regulators, and often already referenced in guidance tied to OCC or NERC CIP expectations. They are also the people who have to explain emerging quantum exposure to executives, boards, and other non-technical stakeholders who want a clear answer: what is at risk, how urgent is it, and what should we do next?

This engagement gives them a defensible, documented answer. It provides evidence they can use in board updates, exam responses, risk committee discussions, and SEC 10-K disclosure preparation, while reducing the burden of translating complex technical findings into business language.

Continuous Validation Option

Extend the engagement into a PTaaS subscription when a one-time assessment is no longer enough. Modern environments change too quickly for annual testing cycles to stay accurate: cloud configurations shift week to week, identity and access paths evolve, and new AI features can introduce entirely new attack surfaces faster than traditional programs can absorb them.

PTaaS keeps the risk register current with ongoing testing cadence, maintained CBOM visibility, AI/LLM continuous coverage, and SLA-backed retesting. That means new findings are validated as the environment changes, not months later, so the team can stay aligned to what is actually exploitable right now.

Our Differentiator: Quantum Security Readiness

Our differentiator is the **quantum security readiness assessment** that is part of every engagement by default. Generalist firms handle TLS configuration and certificate expiry. They do not produce a Cryptographic Bill of Materials, score per-asset Harvest-Now-Decrypt-Later exposure, or correlate offensive findings against quantum-vulnerable algorithms.

OCC Directive

Banks directed to inventory encryption. Examiners already asking about cryptographic inventories.

NIST FIPS 203/204/205

Finalized August 2024. Organizations told to migrate **now**.

NERC CIP FY2025

Audits flagged crypto-agility gaps. Utilities under active scrutiny.

EU AI Act

Red-teaming requirement hits full enforcement **August 2, 2026**. Penalties up to 7% of global revenue.

ⓘ Every one of these regulatory triggers gives a CISO a defensible reason to fund a pen test that does more than confirm the perimeter is reachable.

COMPETITIVE POSITIONING

Generalist vs Quantum Foundry

Capability	Generalist Firm	Quantum Foundry
Manual exploit chaining	Mixed (often junior testers)	Senior-led, attack-path mapped. Valuates strength, correctness, and lifecycle of cryptographic mechanisms
CVSS scoring	CVSS 3.1 base score	CVSS 4.0 with environmental and threat metrics
Cryptographic Bill of Materials	Not offered	Living CBOM, examiner-ready
Quantum vulnerability scoring	Not offered	Per-asset HNDL exposure rating. Identifies weak/obsolete crypto (e.g., RSA-1024, TLS 1.0), improper key management, non-compliance with standard
Linked finding correlation	Not produced	Combined risk register with HNDL flags
Regulatory crosswalks	Partial (PCI, HIPAA, SOC 2)	OCC, NERC CIP, NIS2, SEC, EU AI Act, NIST AI RMF, MITRE ATLAS. Deep inspection of crypto libraries, protocol negotiation, certificate chains, random number generator
Crypto-agility scoring	Not offered	Time-to-rotate scored per system. Algorithms, key sizes, certificate validity, protocol versions, PKI design, crypto agility
Detection engineering validation	Optional add-on	Included; SOC and EDR efficacy reported

Cryptographic Vulnerability Assessment Value

Aspect	Cryptographic Vulnerability Assessment
Threat Perspective	Protects against long-term risks (e.g., "harvest now, decrypt later," quantum computing threats)
Regulatory Value	Meets crypto-specific compliance (PCI DSS, NIST, ISO 27001, GDPR encryption requirements)
Business Impact	Ensures confidentiality, integrity, and authenticity of sensitive data even if systems are compromised
Complimenary	Strengthens the trust layer that secures data

What Makes This Different

1	**Two Workstreams, One Team** Active testing runs alongside a passive cryptographic discovery workstream. Findings from each side are reviewed together at the end of testing so we can flag combined risks — for example, a lateral movement path that exposes seven years of customer data protected by a deprecated cipher.
2	**Senior-Led, Manual-First Delivery** Every engagement is led by a senior offensive engineer with documented experience in the customer's sector. Automated tooling handles reconnaissance and surface enumeration so human testers spend their time on business logic, attack chaining, post-exploitation, and the kinds of findings that scanners do not produce.
3	**Forward-Defensible** The deliverables answer questions a board, an examiner, and an insurer will all ask. The CBOM, quantum exposure register, and executive briefing pack are designed to satisfy regulators referencing OCC December 2024 guidance, NERC CIP-015-1, PCI DSS 4.0, NIS2 Article 21, and SEC cyber disclosure rules.

We do not pursue customers who want the checkbox pen test that passes an audit. The engagement is priced and scoped for organizations with material cryptographic risk and meaningful blast radius.

SECTION 2

What the Pen Test Includes: Workstream A

The engagement covers the offensive baseline that any enterprise should expect, plus the emerging surfaces that most generalist firms cannot reach. Scope flexes based on the customer's environment.

Network & Infrastructure

- External network testing: internet-facing services, firewall rule analysis, exposed admin interfaces
- Internal network testing: lateral movement, segmentation validation, privilege escalation paths
- Active Directory abuse: Kerberoasting, ASREP roasting, ADCS misconfiguration, delegation abuse
- Wireless testing (optional): rogue AP detection, WPA2/WPA3 credential capture

Application Layer

- Web application testing: OWASP Top 10 2021 and OWASP ASVS, business logic abuse, SSRF, auth bypass
- API testing: OWASP API Top 10, broken object-level authorization, injection, excessive data exposure
- Mobile application testing (optional): iOS and Android, OWASP MASVS, certificate pinning bypass
- Source code review (optional): high-risk components, scoped per lines of code

AI Red Teaming

• **Proactively Identify AI Risks** – Uncover vulnerabilities such as prompt injection, data leakage, hallucinations, bias, and unsafe model behavior before they impact your business.

• **Strengthen Security, Compliance & Trust** – Validate that AI systems operate safely, reliably, and in alignment with regulatory requirements, governance frameworks, and organizational policies.

• **Improve AI Resilience Through Adversarial Testing** – Simulate real-world attacks and misuse scenarios to expose weaknesses, implement mitigations, and enhance the security and robustness of AI deployments.

Cloud & Container

- AWS, Azure, GCP: identity and access policy abuse, privilege escalation, exposed storage
- Container and orchestration: Kubernetes cluster review, container escape, supply chain risk
- Serverless function testing: function event injection, IAM scoping flaws

Identity & Access

- Authentication system testing: MFA bypass, session handling, password policy validation
- SSO and federation: SAML and OIDC flaw testing, token replay, audience confusion attacks
- Privileged access management review where deployed

Adversary Emulation

- MITRE ATT&CK-aligned scenarios scoped to sector-specific threat actors
- Detection engineering validation: SOC visibility reporting
- Social engineering (optional): phishing, vishing, physical access

Workstream B: Cryptographic Vulnerability Assessment

This workstream runs in parallel with active testing. It is **passive and non-intrusive** — safe to run in production environments and OT networks where active testing would be prohibited.

The output is a **Cryptographic Bill of Materials (CBOM)** plus a quantum exposure register covering seven domains.

Network Protocols

TLS/SSL versions, cipher suite enumeration, HSTS, PFS, deprecated protocol detection

Public Key Infrastructure

Full certificate inventory: issuer, key length, algorithm, expiry, chain validity, SHA-1/MD5 detection

App-Layer Crypto

Hash algorithm usage, symmetric encryption review, PRNG patterns, password storage, hardcoded key detection

Key Management

HSM configuration, key rotation policy, AWS KMS / Azure Key Vault / GCP KMS review, key custody documentation

Quantum Vuln Scoring

Per-asset HNDL exposure score based on algorithm vulnerability, data confidentiality horizon, and network accessibility

Supply Chain Crypto

API integration cryptography, vendor connection security, SBOM cryptographic dependencies, third-party HSM/KMS exposure

Crypto-Agility Scoring & Standards Alignment

Crypto-Agility Scoring

We score each system on how quickly the customer could swap an algorithm or rotate a key if a vulnerability dropped tomorrow. This is the metric examiners are starting to ask about and that procurement teams are writing into vendor contracts.

A system with hardcoded RSA in firmware scores poorly. A system using a key management service with rotation automation scores well. The score becomes part of the migration roadmap.

Testing Methodology Aligns To

- NIST SP 800-115 (technical guide to security testing)
- PTES (Penetration Testing Execution Standard)
- OWASP Top 10, API Top 10, LLM Top 10, MASVS, ASVS
- OWASP Top 10 for Agentic Applications 2026
- MITRE ATT&CK and MITRE ATLAS
- NIST AI Risk Management Framework
- NIST FIPS 203 (ML-KEM), 204 (ML-DSA), 205 (SLH-DSA)
- CVSS 4.0 with environmental and threat-context modifiers

Four Core Deliverables

1

Penetration Test Report

Every exploitable finding documented with reproducible proof-of-concept, CVSS 4.0 score (base, threat, environmental), prioritized remediation guidance, and attack-chain narrative. Includes a detection-engineering appendix documenting which testing actions produced alerts in the customer's SOC.

2

Cryptographic Bill of Materials

A living inventory of every algorithm, protocol, certificate, and key across the in-scope estate. Each asset carries a quantum vulnerability index, a confidentiality-horizon estimate, and a migration priority tier. Format is examiner-ready and machine-readable (JSON or CycloneDX 1.6).

3

Quantum Readiness & CVA Report

Risk-rated cryptographic findings with HNDL exposure scoring, certificate risk register, regulatory gap analysis (OCC, NERC CIP, PCI DSS 4.0, SEC, NIS2, EU AI Act), and a phased PQC migration roadmap mapped against NIST FIPS 203/204/205.

4

Executive Briefing Pack

Board-ready, 8–12 pages. Traffic-light dashboard, top five findings in plain language, regulatory obligations referenced by name, and a 12-month remediation timeline with budget bands. Designed to satisfy CRO and audit committee questions without requiring the CISO to translate technical content.

Engagement Options

Dimension	Standard	Extended
Organization size	200 to 2,000 employees	2,000 to 10,000 employees
Pen test scope	External, internal, up to 3 web apps, cloud, identity	All Standard plus, up to 8 web apps, social engineering, AI red teaming
CVA scope	Internet-facing TLS, PKI, app crypto, cloud KMS	All Standard and embedded crypto, supply chain, third-party API crypto
Best fit	Regional banks, credit unions, mid-size utilities, payment processors, hospital systems	Tier 1 financials, transmission utilities, pipeline operators, large pharma, defense supply chain

SECTION 4

Remediation: A First-Class Output

Most pen tests stop at the report. That is the largest single complaint enterprise buyers have about the category. We make remediation a first-class output so the customer's engineering team can act on findings without spending weeks translating the report into work tickets.

Severity Tier with Business-Risk Weighting

CVSS 4.0 base score plus environmental modifiers based on the customer's actual deployment. A critical finding on a sandbox does not get treated like a critical finding on the payment gateway. The scoring methodology is documented so engineering teams can defend prioritization to their leadership.

Reachability and Exploitability Validation

Where a finding chains with another, the report shows the chain. Where a vulnerable library is present but the vulnerable code path is not reachable, the report says so. This reduces wasted remediation work — the second-largest complaint enterprise teams have about pen test outputs.

Specific Remediation Steps

Not 'apply patches.' Concrete configuration changes with version targets and code patterns to fix. Where multiple remediation paths exist, we show the trade-offs.

Validation Guidance

How the customer or a third party can verify the fix. For complex findings, we include reproducible commands and scripted validation steps where appropriate.

Compliance Crosswalks

Findings map to the regulatory regimes the customer is accountable to. We embed the mapping inside the findings so the same evidence base supports remediation work and examiner conversations.

Regime	How Findings Map
OCC December 2024	CBOM satisfies the inventory directive. Quantum exposure register supports PQC migration planning evidence in 2025 and 2026 examinations.
NERC CIP / CIP-015-1	Internal network monitoring requirement (June 2025) supported by CBOM. Crypto-agility scoring addresses FY2025 audit gaps.
PCI DSS 4.0	TLS 1.3 verification, SHA-1 prohibition validation, future-dated crypto requirement evidence (mandatory March 2025).
SEC Cyber Disclosure	CVA report provides documented evidence supporting 10-K disclosure of material cryptographic risk.
NIS2 Article 21 (EU)	Cryptographic risk management evidence for essential and important entities subject to supervisory audits.
EU AI Act	Red-teaming evidence for high-risk AI systems, full enforcement August 2, 2026, penalties up to 7% of global revenue.
NIST FIPS 203/204/205	Migration roadmap maps current cryptographic posture to ML-KEM, ML-DSA, and SLH-DSA targets.
CNSA 2.0	NSA algorithm inventory mapping for defense supply chain assets needing migration by 2027.

Extend the value of your engagement with post-delivery advisory hours. Partner directly with your original senior engineer for expert guidance on architecture, remediation, and validation—all through a clear, scoped engagement model.

SECTION 5

Re-Test and Continuous Validation

Re-testing is included in the base engagement. After the customer reports findings remediated, we validate fixes within a **90-day window** from the date the final report is issued.

What Is Included in Re-Test

- Re-testing of every Critical and High finding
- Re-testing of Medium findings on request
- Updated CVSS 4.0 scoring on each re-tested finding
- Attestation letter for regulators, insurers, and auditors
- Refreshed executive summary documenting risk reduction

How Attestation Works

The attestation letter is signed by the engagement's senior lead and references the original report by ID, the specific findings tested, the date of validation, and the methodology applied.

It is the document a CRO hands to a regulator who asks *'were the findings from the December assessment fixed?'* The format aligns to evidence requirements seen in OCC examinations, NERC CIP audits, PCI QSA reviews, and standard cyber insurance underwriting.

Continuous Validation Subscription (PTaaS)

PTaaS is the fastest-growing segment of the pen test market (**22.6% CAGR through 2031**) because enterprise environments now change faster than annual testing can validate. Cloud configurations shift weekly. AI features deploy monthly. Certificate inventories drift between major engagements. New CVEs appear within hours of disclosure.

The Continuous Validation Subscription is positioned as the **standard offering** — not a peripheral add-on. Customers buy the initial engagement first, then move into a continuous subscription with renewable 12-month terms.

What Every Tier Includes

- Customer portal with live finding tracking and remediation status
- Direct messenger access to the assigned testing team during business hours
- Automated reconnaissance with human-led validation of findings
- On-demand retesting of any open finding within a tier-specific SLA
- Compliance crosswalk maintenance (OCC, NERC CIP, PCI DSS 4.0, NIS2, EU AI Act, NIST AI RMF)
- Change-triggered testing for designated critical assets
- Integration with Jira, ServiceNow, and native APIs
- Quarterly CBOM refresh at minimum, with quantum exposure register updates
- Monthly written summary delivered to the security team

Subscription Tiers

Dimension	Foundation	Active	Premier
Best fit	Continuity without heavy testing volume	Regulated sectors with frequent change	Tier 1 enterprises with material AI deployments
Active testing cadence	Quarterly windows	Monthly + change-triggered on critical assets	Continuous, dedicated senior engineer
CBOM refresh cycle	Quarterly	Monthly	Bi Weekly with quantum exposure scoring
Retest SLA	30 days	14 days	7 days
AI/LLM Red Teaming	Optional add-on	Included for production AI features	Included with model-update triggered re-evaluation
Executive briefing	Quarterly written summary	Monthly summary + quarterly call	Monthly call + quarterly board-ready update
Detection engineering	Annual review	Bi-annual exercise	Quarterly team + continuous control efficacy
Attestation letters	2 per year	4 per year	Unlimited within scope
Supply Chain (CVA) Cryptographic Vulnerability Assessment	Identifies cryptographic risks within critical third-party vendors through high-level cryptographic scanning, questionnaires, and documentation reviews.	Evaluates third-party cryptographic exposure through targeted assessments, evidence validation, and risk-based vendor analysis.	Provides comprehensive assessment of third-party cryptographic risks through advanced technical validation, supply chain dependency mapping, continuous monitoring, and strategic remediation guidance.

Why PTaaS Is Core to the Program

Market Expectation

Most enterprise pen test buyers now expect a continuous option as part of any serious vendor relationship. Without one, we lose late-stage procurement deals to NetSPI, Cobalt, Synack, and Bishop Fox — all of whom have mature platforms.

Durable Revenue

Recurring revenue from a continuous subscription is durable in a way that one-off engagements are not. This improves planning, hiring, and capacity utilization across the business.

Strongest Proof Point

The continuous model is where the quantum and crypto-agility story gets its strongest proof point. Customers can see their CBOM and quantum exposure register move over time as remediation progresses — visible progress a CRO will use to defend the program internally.

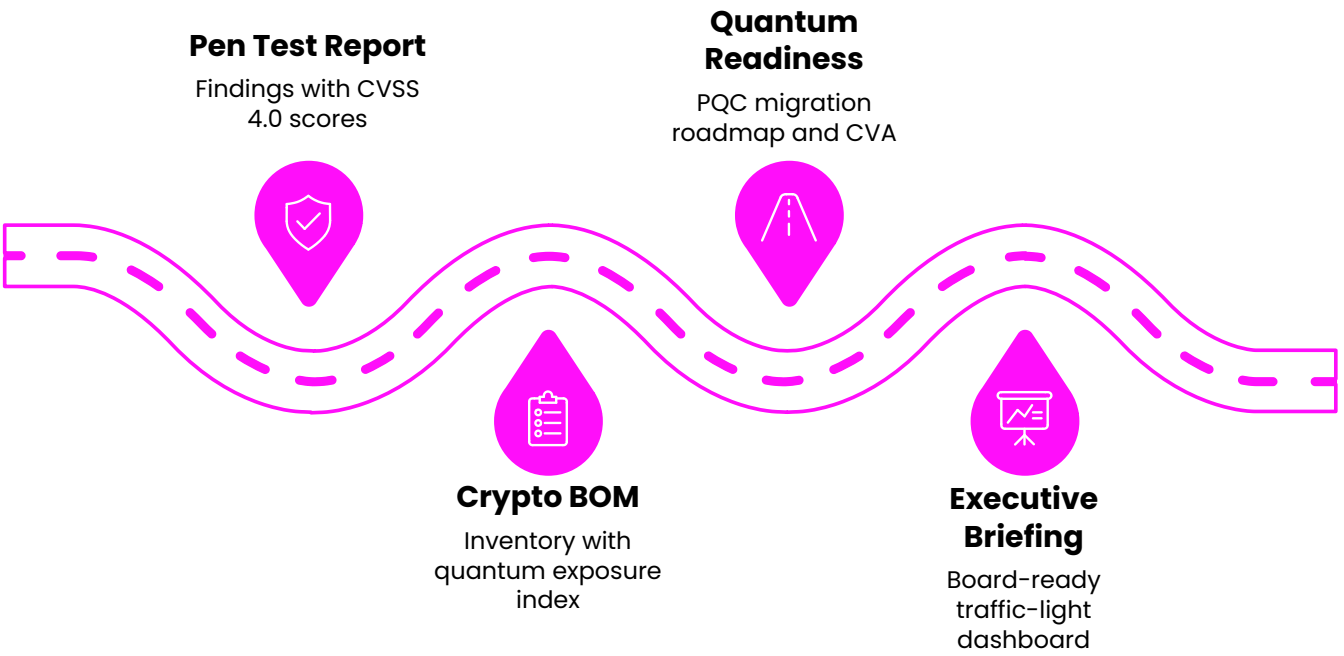
How Customers Move Into the Subscription

1. After the initial engagement readout, the customer receives a subscription proposal scoped to their environment
2. Subscription begins within 30 days of engagement close, with no testing gap
3. First quarterly review at 90 days, including tier evaluation
4. Customers can step up tiers mid-term with a prorated adjustment; step-downs apply at the next renewal
5. Tier Premier customers receive a dedicated senior lead who stays with the account across renewals where capacity allows

SECTION 6

Summary

Quantum Foundry runs a single offensive security engagement that finds what is exploitable in your environment today and produces the cryptographic evidence base your regulators, auditors, and insurers will all eventually ask for. Delivery is senior-led and manual-first, scoped for large enterprises in regulated, high-stakes sectors. The engagement combines deep penetration testing with a quantum security readiness assessment under one statement of work, one team, and one correlated risk register. The output is four deliverables — pen test report, Cryptographic Bill of Materials, quantum readiness report, executive briefing pack — plus an included re-test cycle and a continuous validation subscription.



Why Act Now

Regulatory Windows Are Closing

OCC December 2024 directed banks to inventory encryption. PCI DSS 4.0 future-dated requirements went mandatory March 2025. NERC CIP-015-1 went into effect June 2025. EU AI Act full enforcement August 2, 2026. NIST published final PQC standards August 2024 and tells organizations to migrate immediately.

Adversaries Are Collecting Now

Harvest-Now-Decrypt-Later attacks are happening. Nation-state actors are storing encrypted data they cannot read today against the day quantum computers can. Any data with a confidentiality horizon longer than five to ten years is already at risk.

Discovery Alone Takes time

AppViewX research and GRI/evolutionQ analysis both put cryptographic discovery at one to two years for a large enterprise before migration even starts. Organizations waiting until 2028 face compressed, high-risk transitions.

Add-On Modules

CBOM Refresh (Annual)

Keeps the cryptographic inventory current for customers not on a continuous subscription. Captures certificate churn, new TLS endpoints, and key management changes.

Third-Party Vendor CVA

Addresses OCC guidance to assess vendors' PQC transition plans. Critical for organizations with complex supply chains.

Regulatory Readiness Review

Pre-examination evidence pack mapped to NERC CIP, OCC, PCI QSA scope. Delivered before scheduled audits.

PQC Migration Roadmap (Deep)

Phased migration plan from current posture to NIST FIPS 203/204/205 compliance. Full architecture-level guidance.

AI/LLM Red Team (Deep)

Standalone follow-on for customers with material AI deployments. Covers OWASP LLM Top 10 and Agentic Applications 2026. A comprehensive adversarial testing service that identifies AI vulnerabilities, validates security and compliance controls, and strengthens the resilience, safety, and trustworthiness of AI systems against real-world threats and misuse scenarios.

Remediation Advisory Hours

Senior engineer time sold in 20-hour blocks for fix validation review and architecture guidance on the most complex findings.

From First Call to Final Report

The path from initial conversation to completed engagement is designed to be fast, transparent, and low-friction for the customer's team.

01

Discovery Call

Scope context, sector regulatory exposure, quantum risk horizon. No preparation required from the customer.

02

Technical Scoping Session

In-scope systems, testing windows, AI surfaces, third-party crypto exposure. Includes detailed scoping workshops for the cryptographic vulnerability assessment — built into the billable contract.

03

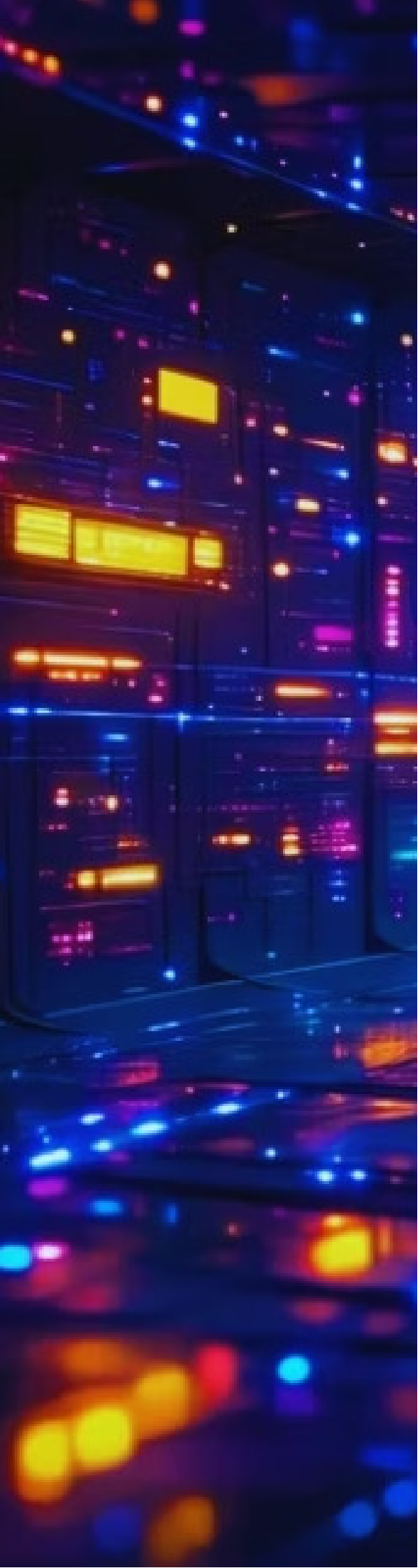
Proposal and Statement of Work

Issued within five business days of the technical scoping session. Includes engagement scope, timeline, deliverables, and subscription proposal.

04

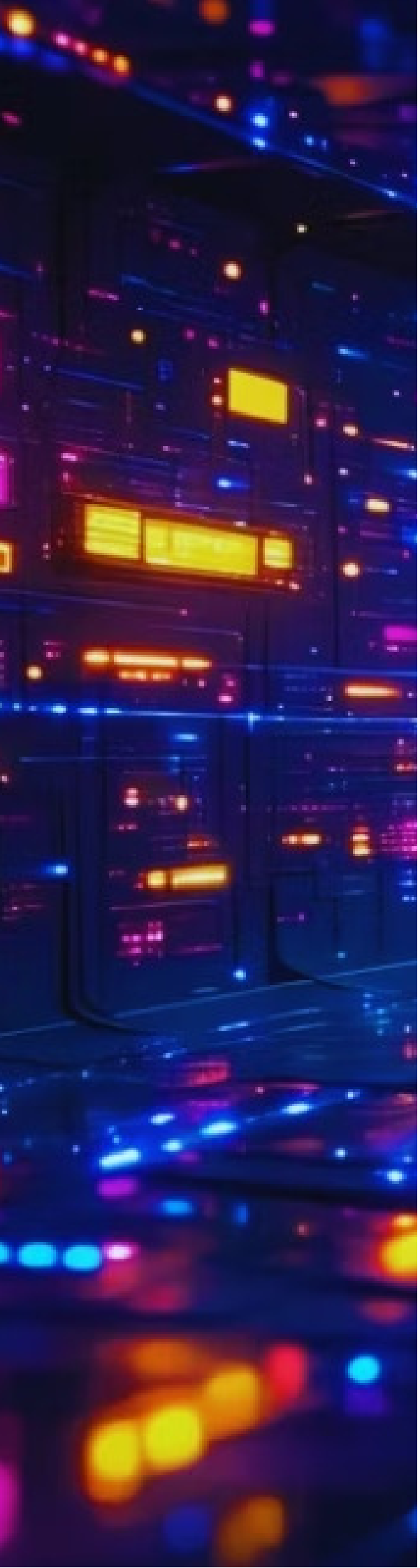
Kickoff

Rules of engagement signed. Engagement begins. Passive CVA discovery starts in week one.



Quantum Foundry

CYSTEL



Appendix

ENTERPRISE BUYER INTELLIGENCE

Enterprise Trends for 2026

Enterprise security leaders have moved past treating pen tests as annual PDFs. They expect findings that flow into ticketing systems, get retested, and prove control effectiveness on a cadence the threat environment justifies.

Continuous Validation, Not Point-in-Time Tests

PTaaS revenue growing at 22.6% CAGR. CISA urged quarterly testing for critical infrastructure after the 2025 Polish energy grid attack. Median testing budgets reached **$187K**. Buyers want a base engagement plus ongoing testing cadence.

Senior-Led Manual Depth

Buyers explicitly distinguish between scan-heavy delivery and human-led attack chaining. Boutique firms ranked highly in 2026 procurement guides because senior testers chain findings, validate exploitability, and surface business logic flaws scanners cannot reach.

Attack-Path Validation Over Vulnerability Lists

Enterprises want proof of how an attacker moves through the environment — not a CVSS-sorted spreadsheet. Reports that map kill chains and tie technical findings to business impact win procurement.

Cloud-Native Attack Surface Depth

Cloud security pen testing is the fastest-growing PTaaS segment at **25.8% CAGR**. Buyers expect testing of containers, serverless, identity privilege paths, multi-cloud KMS, and exposed APIs. 61% of organizations had a cloud security incident in the past year.

Multi-Audience Reporting and Integration

CISOs need three things from one engagement: technical findings their engineers can reproduce, executive briefings their board will absorb, and compliance crosswalks their auditors and insurers will accept. Reports that ship as static PDFs are losing to platforms that integrate with Jira, ServiceNow, and vulnerability management tools.

The Hidden Risk: Data, AI, and Cryptography

Right now, most organisations treat data, AI, and cryptography as **separate domains**. That separation is exactly where the risk lives.

Modern AI systems are powered by vast volumes of sensitive data — customer records, financial transactions, intellectual property. This data is constantly in motion: collected, shared, processed, and stored across distributed environments. Cryptography is what's supposed to protect it at every stage. But in practice, cryptographic controls are often inconsistent, outdated, or poorly governed.

AI Accelerates the Problem Two Ways

1. It increases the value and exposure of data — making it a more attractive target.

2. It introduces new attack surfaces where encrypted data is decrypted, transformed, or reused in ways that bypass traditional controls.

Advances in AI are enabling more sophisticated threat actors to discover weaknesses in encryption implementations faster than ever.

⚠ The result is a growing class of cryptographic vulnerabilities invisible to traditional security assessments: weak key management, deprecated algorithms, hardcoded secrets, and misconfigured encryption across AI pipelines and data ecosystems.

COMPETITIVE GAP ANALYSIS

What Is Missing From Most Enterprise Pen Tests

Three gaps appear in nearly every competitive analysis reviewed. Each one is a place we can build a deliverable that competitors cannot match without a meaningful pivot.

Algorithm-Level Cryptographic Visibility

Standard pen tests check TLS versions and flag expired certificates. They do not produce a Cryptographic Bill of Materials, do not score quantum exposure, do not assess key management, and do not map to NIST FIPS 203/204/205.

The seven CVA domains — network protocols, PKI, application crypto, key management, quantum scoring, embedded/OT crypto, supply-chain crypto — all sit in our scope.

Linked Finding Correlation

A medium-severity lateral movement finding plus a high-severity quantum-vulnerable cipher protecting seven years of customer data is a **critical Harvest-Now-Decrypt-Later finding**.

No generalist firm produces that correlated risk register because they run pen tests and crypto reviews as separate engagements with different teams. We do it in one.