Post-Quantum Readiness Report: Example Outfitters (sample)

Demo data. Example Outfitters is a fictional company; all hosts, certificates and findings are simulated.

Quantinus

EXECUTIVE RISK BRIEFING - POST-QUANTUM CRYPTOGRAPHY ASSESSMENT

Tenant: Example Outfitters (Demo)

November 17, 2026

CONFIDENTIAL

D

HYGIENE GRADE

WEAK POSTURE

7%

QUANTUM-SAFE COVERAGE

EARLY

Limiting factor: **Hygiene grade** — 3 unresolved critical findings in classical posture

POST-QUANTUM EXPOSURE

26 post-quantum blockers on 22 hosts. Traffic these systems protect can be recorded today and decrypted once a quantum computer can break its key exchange, and certificates on RSA or ECDSA keys that are still valid then could be forged.

EXPOSURE	HOSTS
SSH sessions use key exchange with no post-quantum option.	14
TLS connections use classical key exchange only.	6
Certificates on quantum-vulnerable keys stay valid for years.	4
TLS uses static RSA key exchange: whoever later obtains the server key, by theft or by quantum computer, can decrypt every recorded session.	1

WHAT TO FIX FIRST

The first three items on the remediation roadmap: security gaps first, then critical and high findings, then post-quantum blockers. The technical report has the steps for each host.

#	RISK	FIX FIRST	HOSTS
1	**An SSH server proves its identity with a DSA key, an algorithm OpenSSH has deprecated and removed.** CRITICAL	Replace the DSA host key with an Ed25519 key.	1
2	**Certificates use RSA keys below the current minimum size.** HIGH	Reissue them with new RSA-3072 or ECDSA P-256 keys and revoke the old certificates.	8
3	**SSH servers prove their identity with RSA keys below the current minimum size.** HIGH	Add an Ed25519 host key, or regenerate the RSA key at 3072 bits or more.	9

Certificate expiry: 2 expired and 2 expiring within 90 days. The Certificate Expiry report lists every date.

20	130	3	26	0%
TOTAL SCANS	TOTAL FINDINGS	CRITICAL	PQ BLOCKERS	COMPLIANCE

RISK DISTRIBUTION

Critical	3	
High	41	
Medium	33	
Low	4	
Info	49	

FINDING TAGS

PQ Blockers	26
PQ Signals	18
Agility Gaps	5
Security Gaps	50
Informational	31

ALGORITHM EXPOSURE

RSA-1024	39
RSA-2048	30
SHA256-RSA	26
Ed25519	10
SHA1-RSA	7
secp256r1	5
DSA	5
TLS_RSA_WITH_AES_128_CBC_SHA	4