



## Cerebion Rivet — Quick Reference Card

---

### Before You Scan

Always work on a **copy or dedicated branch** — never apply AI-generated fixes directly to production systems or your main branch. Review all fixes before committing.

---

### Risk Score Guide

| Score  | Level    | Action                          |
|--------|----------|---------------------------------|
| 0–25   | Low      | Monitor; no immediate action    |
| 26–50  | Medium   | Plan migration within 3–5 years |
| 51–75  | High     | Prioritize migration now        |
| 76–100 | Critical | Begin migration immediately     |

**Score = Algorithm Risk (40%) + Timeline Risk (25%) + Business Impact (20%) + PQC Readiness (15%)**

---

### Algorithm Risk at a Glance

| Algorithm          | Score    | Status                                          |
|--------------------|----------|-------------------------------------------------|
| RSA-1024           | 95       | Critically vulnerable — breakable by 2026–2028  |
| RSA-2048           | 88       | Highly vulnerable — breakable by 2032–2035      |
| ECDSA P-256 / ECDH | 90       | Fewer qubits needed than RSA — equally critical |
| DSA / DH           | 40 (max) | Fully broken by Shor's algorithm                |
| AES-128            | 30       | Grover halves security to 64-bit                |
| MD5 / SHA-1        | 100      | Classically and quantum broken                  |
| AES-256 / SHA-384+ | 0        | Quantum-resistant                               |

---

### Post-Quantum Replacements (NIST FIPS)

| Replace              | With                                 | Standard |
|----------------------|--------------------------------------|----------|
| RSA-OAEP / ECDH / DH | <b>ML-KEM</b> (Kyber)                | FIPS 203 |
| RSA / ECDSA / DSA    | <b>ML-DSA</b> (Dilithium)            | FIPS 204 |
| ECDSA (stateless)    | <b>SLH-DSA</b> (SPHINCS+)            | FIPS 205 |
| AES-128              | <b>AES-256</b> / ChaCha20-Poly1305   | —        |
| SHA-1 / MD5          | <b>SHA-384</b> / SHA-512 / SHAKE-256 | —        |

---

## Quantum Threat Timeline

| Year | Threat Level | At Risk                               |
|------|--------------|---------------------------------------|
| 2024 | Minimal      | No cryptographic attacks              |
| 2026 | Low          | RSA-512, ECC-160, weak DH             |
| 2032 | Medium       | RSA-2048, ECDSA P-256, DH-2048        |
| 2037 | High         | RSA-4096, ECDSA P-384, DH-4096        |
| 2040 | Critical     | All classical public-key cryptography |

---

## Supported Binary Formats

PE (.exe, .dll) · ELF · Mach-O (.dylib, .app) · .NET · Java .class / JAR · DEX (Android)

---

## Supported Code Languages

46 languages and configuration formats, including: Python · JavaScript · TypeScript · Java · C/C++ · C# · Go · Rust · Ruby · PHP · Kotlin · Scala · Swift · Bash · Lua · Perl · PowerShell · R · VB · COBOL · Groovy · Apex · Elixir · Clojure · OCaml · Scheme · Vue · Dart · Solidity · Cairo · Circom · Move · Terraform · HCL · Dockerfile · SQL · JSON · YAML · TOML · XML · Jsonnet · .env · Protocol Buffers

---

## Key Management Analyzer (Beta) — Supported Backends

HashiCorp Vault · AWS KMS · AWS Certificate Manager · Azure Key Vault · Azure Managed HSM · GCP Cloud KMS · Kubernetes Certificate Manager (cert-manager) · Microsoft AD CS

Requires a read-only, customer-issued credential per backend. Credentials are stored only in your OS credential manager (never in Rivet's database, never sent to Cerebion), and the connector cannot decrypt, sign, or export — read-only by design. On-premise only.

---

## Binary Analysis Confidence Levels

| Confidence | Meaning                               |
|------------|---------------------------------------|
| High       | YARA + binary analysis both succeeded |
| Medium     | One method succeeded                  |

| Confidence   | Meaning                                                        |
|--------------|----------------------------------------------------------------|
| YARA Primary | YARA matched; binary analysis limited (stripped/packed binary) |
| UNKNOWN      | No analyzable content found                                    |

## Q-Score Reference (YARA Rules)

| Q-Score | Severity | Examples                                  |
|---------|----------|-------------------------------------------|
| 5       | CRITICAL | RSA, ECDSA, ECDH, DH, AES-128, MD5, SHA-1 |
| 4       | HIGH     | Weak PQC params, PRNG in crypto context   |
| 3       | MEDIUM   | Legacy crypto in quantum-aware systems    |
| 2       | LOW      | Performance-mode PQC, debug code          |
| 1       | INFO     | Migration recommendations                 |

## Reports Page

Select analyses from the Scan History table (latest per target shown), add optional context, and click **Generate Report**. Reports are saved to the database and available for download (Markdown or HTML) at any time. Delete reports you no longer need.

## AI Features (Settings → AI & LLM Configuration)

| Feature                     | What it does                                                                                                                       |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>AI Report Generation</b> | Generates executive summary reports on the Reports page based on selected analyses and user context                                |
| <b>AI Fix Generation</b>    | Suggests fixes for code findings — choose Comment annotation (safe, non-destructive) or Code generation (replaces vulnerable code) |

## Key Settings Locations

| What                       | Where                              |
|----------------------------|------------------------------------|
| License                    | Settings → License                 |
| Binary limits              | Settings → Binary Analysis         |
| Code scan extensions       | Settings → Code Analysis           |
| AI API key & features      | Settings → AI & LLM Configuration  |
| Network port range         | Settings → Network Analysis        |
| Key Management connections | Key Management page (not Settings) |
| Log level                  | Settings → Application             |

## Environment Variables

---

| Variable             | Purpose                                   |
|----------------------|-------------------------------------------|
| RIVET_LICENSE_KEY    | License key for headless/CI activation    |
| OFFLINE_LICENSE_FILE | Path to offline license file (air-gapped) |

---

## Log Locations

---

| Platform | Path                                      |
|----------|-------------------------------------------|
| Windows  | %APPDATA%\CerebionRivet\logs\app.log      |
| macOS    | ~/Library/Logs/CerebionRivet/logs/app.log |
| Linux    | ~/.config/CerebionRivet/logs/app.log      |

---

## Important Limitation

The Binary Analyzer performs **static analysis only**. A clean result means no known vulnerable patterns were detected — it does not guarantee the binary is quantum-safe. Runtime-only crypto, custom implementations, and encrypted/packed sections are outside detection scope.

---

**Version** 1.1.92 · **Support:** support@cerebion.com · **Docs:** cerebion.com/docs · **Portal:** cerebion.com/portal