OnDefend

Cryptography & Post Quantum Prep Assessment

Eliminate Hidden Cryptographic Attack Paths

Adversaries exploit weak encryption and poor key management to silently reach your most sensitive data. Harvest-now-decrypt-later attacks mean quantum-vulnerable data is already being collected today.

OnDefend combines AI-powered attack simulation with elite operators to expose cryptographic attack paths and the fixes that collapse them.

Testing Capabilities

Network & Transport Encryption

Tests TLS/SSL configurations, certificates, and cipher suites for weaknesses exposing data in transit.

APIs & Token-Based Systems

Tests JWT handling, token signing, and validation logic to prevent tampering and unauthorized access.

Post-Quantum Cryptography Readiness

Identifies quantum-vulnerable algorithms, crypto-agility gaps, and harvest-now, decrypt-later exposure.

Key Management & Cryptographic Usage

Validates key generation, storage, rotation, and access controls across systems and trust relationships.

Weak & Deprecated Algorithm Detection

Identifies outdated algorithms such as MD5, SHA-1, and weak RSA that can be broken or bypassed.

Token & Session Security

Tests token signing, validation, and expiration logic to prevent impersonation and session hijacking.

Outcomes

- Weak cipher suites, key failures, and quantum-vulnerable algorithms identified and prioritized
- Prioritized findings with severity ratings, affected systems, and remediation steps
- Cryptographic attack paths eliminated *(not just flagged)* with architecture-level fixes
- Post-quantum readiness assessed and harvest-now, decrypt-later exposure quantified

By fusing AI-powered attack simulation with elite operators, we expose cryptographic attack paths and pinpoint the algorithm and architecture fixes that collapse them.

OnDefend.com