# Technical Capabilities

Eight core domains, each grounded in direct engineering practice, supported by a closed-loop secure development lifecycle applied to every engagement.

## CORE TECHNICAL CAPABILITIES

### Secure Software Engineering
Security requirements integrated into design, development, and deployment — a design constraint from the start, not a gate at the end.

### Application Security
Architecture review, threat modeling, and vulnerability assessment across web and application platforms.

### DevSecOps
Security controls and automated testing embedded directly into CI/CD pipelines — run on every change, not on a schedule.

### Vulnerability Research
Structured, hands-on research to identify previously unknown vulnerabilities in complex or opaque software.

### Mobile Security
Hands-on engineering assessment of mobile application risk — beyond what automated scanning alone can surface.

### Cloud Security
Configuration and architecture review for cloud-hosted infrastructure and mission systems.

### Reverse Engineering
Analysis of compiled software and firmware to establish behavior and risk when source access is limited or unavailable.

### Defensive Engineering
Design and implementation of controls that reduce attack surface and limit impact when prevention fails.

## SECURE DEVELOPMENT LIFECYCLE

1. **Threat Modeling** — Identify what could go wrong before code is written.
2. **Architecture Review** — Validate design against the threat model.
3. **Code Review** — Structured review for secure coding patterns.
4. **Testing** — Static and dynamic testing exercise real behavior.
5. **CI/CD Integration** — Security gates run automatically on every change.
6. **Continuous Improvement** — Findings feed back into the next design cycle.

*Stage 6 feeds back into Stage 1 — the cycle repeats with each release, not once per program.*