DEMONIC BINARY

ENGINEERING & DEFENSIVE CYBERSECURITY / GOVERNMENT & ENTERPRISE BUYERS

Secure mobile systems. Malware investigation. Evidence-led engineering.

California-based, founder-led engineering practice evaluating scoped enterprise and eligible public-sector work. Every engagement is contingent on verified staffing, authorization and contractual security requirements.

Contact info@demonicbinary.com | +1 (650) 397-1782 | demonicbinary.com

FOCUSED TECHNICAL CAPABILITIES

Mobile security & device trust
Native iOS/Android, authentication, Keychain/Secure Enclave, Android integrity, session lifecycle, secure storage and backend enforcement review.

Defensive malware & binary analysis
Scoped suspicious-code triage, static analysis, bounded reverse engineering, persistence hypotheses and defender indicators with evidence limitations.

Detection engineering & security validation
Authorized assessments, synthetic test scenarios, detector validation, prioritized findings and repeatable remediation/retest criteria.

Backend, API & platform security
REST/API authorization, protected service workflows, release integrity, operational observability, failure analysis and secure engineering changes.

THREE STARTING WORK PACKAGES

01. Malware triage
Scoped evidence inventory, behavioral investigation, indicator pack and containment/revalidation recommendations.

02. Mobile & embedded threat review
Authorized code/device analysis, trust-boundary findings, ranked mitigations and testable acceptance criteria.

03. Detection engineering sprint
Bounded hunt hypotheses, reviewed detection rules, synthetic/approved tests and analyst handoff.

Delivery model
Technical discovery, written scope, approved environment, implementation/review, verification, documented handoff. Fees and timing quoted per project.

INSPECTABLE PUBLIC EVIDENCE

Reproducible demo: demonicbinary.com/research/malware-lab — eight synthetic endpoint events, false positives/negatives, mobile manifest review and source-backed tests.

Other references: demonicbinary.com/projects • /security/sample-deliverables • /engineering-proof. Research examples and synthetic reports are **not** government contract performance.

PROCUREMENT AND COMPLIANCE STATUS — TO VERIFY

Legal structure: Demonic Binary is an owner-reported DBA/sole proprietor; current legal records and signatory require verification. C-corp formation is planned, not completed.

SAM / UEI / CAGE: No active identifiers or registration status verified. No small-business certification, active federal contract or security clearance claimed.

NAICS candidates: 541511, 541512 and 541519; subject to principal activity and buyer-specific review.

Data handling: No authorized FCI/CUI/classified enclave claimed; FAR 52.204-21 and applicable NIST/DFARS requirements are pending contract-specific assessment.

INTERNATIONAL DEFENSE BOUNDARY

Foreign-defense inquiries require end-user and sanctions screening, data classification and ITAR/EAR assessment, with DDTC/BIS authorizations where required before controlled services or technical-data transfer. No unconditional foreign-defense eligibility is asserted.

Buyer resources: demonicbinary.com/government-defense/capability-statement | /government-defense/teaming | /enterprise/security-assurance

PUBLIC CAPABILITY OVERVIEW · NOT A GOVERNMENT CERTIFICATION