Stephenson Stellar Corporation

Title: Vulnerability Assessor **Position ID:** 2026-0007	**Type Position:** Full Time **Level:** PL4
Primary Location: To be determined	**Travel Required:** 20% CONUS and HI
Alternate Location: Home office anywhere in USA	**Contact:** Technical: aechevarria@stephensonstellar.org (Axel Echevarria) Human Resource: bmoyer@stephensonstellar.org (Barb Moyer)

Company Background: Stephenson Stellar Corporation (Stellar) is a nonprofit research and development organization focused on assuring our nation remains a global leader in the Space Domain. Our mission is to foster technological innovation and provide secure space-based solutions.

Stellar is an equal opportunity employer, and all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, national origin, age, disability status, protected veteran status, or any other characteristic protected by law.

Additional information at: www.stephensonstellar.org

Job Description: In this position, you will serve as a Vulnerability Assessor for the Space Systems Protection Directorate. You will be required to execute technical offensive security assessments for government and military customers. This role leverages penetration testing and reverse engineering that requires seasoned technical leadership, deep hands-on skills, and the ability to translate findings into actionable remediation and risk reports for system owners. Candidates should be fluent in adversary emulation, exploit development, binary analysis, firmware and software reverse engineering, and common pen testing tool chains. Additional responsibilities include: (1) Plan, scope, and lead complex vulnerability assessments and penetration tests of space vehicle and support systems, including traditional information systems, cloud based systems, network, host, embedded, application, RF/telemetry, and vehicle architecture; (2) Perform hands-on red team / adversary emulation engagements that include reconnaissance, privilege escalation, lateral movement, persistence, and data-exfiltration scenarios tailored to mission system architectures; (3) Reverse engineer firmware, device binaries, software components, and proprietary protocols to discover logic flaws, hidden functionality, or exploitable vulnerabilities (static and dynamic analysis); (4) Develop and test proof-of-concept exploits, custom tooling, fuzzers, and automation to validate high-impact findings and demonstrate risk to stakeholders; (5) Produce high-quality deliverables including Test Plans, Exploitation & Findings Reports, Risk/Impact Analyses, Remediation Recommendations, and executive briefings suitable for Authorizing Officials; (6) Integrate assessment outputs with government authorization workflows and evidence systems (e.g., eMASS) and contribute findings into SARs, POA&Ms, and continuous monitoring processes; (7) Mentor and lead junior assessors and testers; perform quality reviews of technical findings and test methodologies; and (8) Keep current with threat-actor techniques, tooling, and published vulnerabilities; contribute to internal research and reusable toolsets.

Requirements

Clearance: Ability to maintain a Top-Secret clearance.
Citizenship: Candidate must be a United States citizen.
Education:

- BS in Computer Science, Computer Engineering, Cybersecurity, Electrical Engineering.
- An advanced degree is preferred.

Experience:

- 7 plus years of progressive, hands-on experience in vulnerability assessment, penetration testing or reverse engineering.

Required Skills:

- Experience with DoD/government/aerospace environments.
- Expertise in reverse engineering tools and techniques, (IDA Pro / Ghidra, Radare2, Binary Ninja, ltrace/strace, WinDbg/GDB, QEMU), firmware unpacking, and protocol analysis.
- Proficiency in exploit development and offensive tooling, (Metasploit, Burp Suite, custom Python/Go/Rust tooling, fuzzers (ffuf)), and network/web exploitation frameworks.
- Strong programming/scripting skills in languages such as Python, C/C++, assembly (x86, ARM), and scripting (Bash/PowerShell). Ability to read and modify source code and build small remediation/proof-of-concept tools.
- Experience testing embedded systems, firmware, or devices is highly desirable (ground-station equipment, communications gear, RTOS-based firmware).
- Strong written and verbal communication skills; ability to present technical findings to non-technical leadership and to produce clear, prioritized remediation plans.

Desired Skills:

- Industry certifications: OSCP, OSCE, CREST CRT, GPEN, GXPN, CISSP, or equivalent.
- Prior experience with formal red-team exercises or OPFOR roles in DoD/IC contexts.
- Familiarity with RMF, NIST SP 800-53/53A, NIST SP 800-37, DISA STIGs, and embedding pentest results into A&A artifacts; experience with eMASS or similar GRC/ATO tools preferred.
- Experience with secure development lifecycle reviews, code audits, and supply-chain risk assessments.
- Prior experience participating in accreditation or audit activities (auditor/assessor role).