Leon Johnson

andrew.leon.johnson@gmail.com |Download PDF | Oakland, California 94619

Professional Summary

Security leader with 20+ years building and scaling security programs, from hands-on technical assessments to executive risk communication. Track record of growing teams (4 to 50+ consultants), establishing risk assessment methodologies, and pioneering AI security research. Combines deep offensive security expertise with cross-functional collaboration across legal, compliance, and engineering to drive enterprise risk decisions. Demonstrated ability to identify critical vulnerabilities and translate technical risks into actionable business recommendations. (https://sholuv.net/audio/Leons_Resume_Podcast.mp3)

Experience

Offensive Privacy Lead — October 2024 - Current

TikTok, Mountain View, CA

- Lead enterprise privacy risk assessment programs, identifying and quantifying risks across infrastructure, web, and mobile platforms.
- Manage and develop a team of security engineers, coordinating cross-functionally with legal, compliance, engineering, and product teams on risk decisions.
- Conduct hands-on offensive privacy assessments.
- Develop SOPs, rules of engagement, and testing frameworks aligned with MITRE ATT&CK, NIST, and OWASP standards.
- Develop executive-level risk reporting and communicate findings to technical and executive stakeholders, driving remediation priorities and risk acceptance decisions.
- Enhanced testing methodologies to improve organizational privacy protections and align with regulatory frameworks like CCPA and COPPA.

AI Security Lead / Risk Researcher — November 2023 - September 2024

RunSybil, San Francisco, CA

- Led AI-specific security risk assessments across ML pipelines, identifying critical vulnerabilities in model security, training data integrity, and inference endpoints—75% revealed findings requiring immediate remediation.
- Automated 80% of processes and attack vectors using Large Language Models (LLMs).
- Developed risk quantification frameworks for novel AI attack vectors including prompt injection, model extraction, and data poisoning.
- Advised executive teams on AI security risk posture and remediation priorities; developed offensive tooling for AI security testing.

Principal Security Consultant / Manager January 2011 - August 2023

Rapid7, Remote

- Built and scaled security consulting practice from 4 to 50+ consultants (1,150% growth), establishing risk assessment methodologies, training programs, and service delivery standards for Fortune 100 clients.
- Established security program maturity assessments and risk reporting frameworks; created training curricula later productized as certification offering.
- Developed software for writing detailed assessment reports and recommendations.
- Designed, developed, and implemented multiple lines of business for Rapid7.
- Created security tools, processes, procedures, and content for Rapid7 and clients.
- Led hiring, mentorship, and career development for consulting team; developed Mr. Robot CTF for technical interviews; enabled sales with executive presentation content.

Senior Security Consultant January 2007 - December 2010

Texas Department of Information Resources (DIR), Austin, Texas

- Performed penetration assessments of networks and systems owned and operated by the state of Texas.
- Took a leadership role in the onboarding of new members to organizational security practices and provided necessary training.
- Developed software for DIR to write reports detailing assessment findings and recommendations, reducing report writing times by 50%.

Information Security Analyst July 2004 - January 2007

Center for Infrastructure Assurance and Security (CIAS), San Antonio, Texas

- Tested and evaluated third-party security products.
- Performed setup, maintenance, and security of multi-operating system/networks.
- Facilitated community cyber security awareness tabletop exercises for first responders and community leaders.
- Created and maintained all software programs used in National Cyber Defense Competitions.
- Prepared and taught classes on Information Technology.

CVEs

CVE-2026-28279	High (8.4)	OS Command Injection in osctrl-admin. Authenticated admin injects shell commands via hostname parameter; commands execute as root/SYSTEM on all enrolling endpoints. Co-discovered with Kwangyun Keum @ TikTok USDS.
CVE-2026-28280	High (8.7)	Stored XSS in osctrl-admin query list. Low-priv user injects persistent JavaScript; chainable with CSRF for privilege escalation and full platform compromise. Co-discovered with Kwangyun Keum @ TikTok USDS.

Skills

- Security Risk Assessment
- Team Leadership & Development
- Machine Learning
- AI/ML Security
- Python Programming
- Executive Risk Reporting
- Risk Governance & Frameworks
- Natural Language Processing

Education

BS, Computer Science - The University of Texas at San Antonio June 2005

BA, Psychology - The University of Texas at San Antonio June 2005

Speaking & Publishing

28+ conference talks, panels, and media appearances on offensive security, social engineering, AI risk, and supply chain security. Venues include RSA Conference, BSides, Rapid7 UNITED Summit, Forrester Forums, and podcasts (Layer 8, Security Ledger). Full list at sholuv.net/work.html

Certifications

- OSCP - Offensive Security Certified Professional, 01/01/15, Active
- CISSP - Certified Information Systems Security Professional, Inactive
- NSA IAM - INFOSEC Assessment Methodology National Security Agency, Active
- NSA IEM - INFOSEC Evaluation Methodology National Security Agency, Active
- CEH - Certified Ethical Hacker, 01/01/07, Inactive