STEVE PARK

Email: Steven.EA.Park@Gmail.com **LinkedIn:** www.linkedin.com/in/stevepark-security

SUMMARY

Experienced cybersecurity leader with deep expertise in offensive security operations, red team management, and adversary simulation. Proven success in leading blended security engineering and analyst teams to deliver enterprise-wide security solutions, identifying and prioritizing highest-risk threats through detailed threat modeling, and implementing scalable platforms that balance security, cost, and operational agility. Skilled in planning and executing complex engagements, delivering actionable findings to technical and executive audiences, and developing custom tools, scripts, and training content to enhance security capabilities.

PROFESSIONAL EXPERIENCE

Amerivet – Director of InfoSec; Remote *Feb 2024 – Present*

- Led cross-functional Security Engineering, Analyst, and IT teams to implement SIEM, SOAR, EDR, Vulnerability Management, and other enterprise-wide security solutions.
- Identified and prioritized critical security risks, building threat models and delivering targeted solutions that enhanced resilience across over 220 clinics.
- Balanced security, operational cost, and user experience to ensure secure growth while meeting business agility needs.
- Planned and executed offensive security initiatives, including vulnerability assessments, simulated attack scenarios, and penetration testing.
- Developed and updated security policies and operational playbooks to standardize remediation and ensure compliance.
- Delivered executive briefings and technical reports on engagement results, attack paths, and remediation strategies.

Endpoint Closing – Director of InfoSec; Remote *Mar 2022 – Feb 2024*

- Directed a blended security engineering and analyst organization, deploying EDR, SIEM, and CSPM tooling to improve enterprise-wide security posture.
- Conducted risk assessments to identify and address highest-impact threats, integrating results into long-term security strategy.
- Enhanced vulnerability detection by 40% and improved incident response speed by 25% through optimized processes.
- Led investigations into major incidents and financial fraud, delivering findings and recommendations to executives.
- Collaborated with leadership to align security roadmaps with business and operational priorities.

Squarespace – SOC Engineering Manager; Remote *Jan 2020 – Mar 2022*

- Managed SOC engineering and analyst teams to deliver detection, response, and risk mitigation capabilities.
- Balanced the integration of security controls with development velocity in a high-growth environment.
- Built and deployed enterprise-scale EDR, SIEM, and CSPM solutions to address priority threats.
- Led detection engineering projects focused on high-risk scenarios, improving detection and reducing response time.
- Partnered with engineering to embed security into the product lifecycle without introducing excessive friction.

Autodesk – Red Team Manager Offensive Security; Remote *Mar 2017 – Jan 2020*

- Managed global red team engagements, leading a distributed team to identify and address high-priority vulnerabilities.
- Created detailed threat models for high-value assets, driving remediation efforts that strengthened cloud security by 60%.
- Facilitated remediation while balancing technical solutions with operational priorities.
- Applied IoT, embedded systems, and VPN expertise in attacker-modeled penetration testing with custom-built tools.

NCC Group – Senior Security Engineer; Austin, Tx *Jan 2014 – Mar 2017*

- Led penetration tests for Fortune 500 clients, prioritizing vulnerabilities based on highest business risk.
- Spearheaded a coordinated vulnerability disclosure program, reducing exposure to zero-day threats.
- Founding member of the digital forensics and incident response team.
- Earned CVE (CVE-2017-6701) for NAC bypass and privilege escalation exploit.

US Marine Corps – Special Operations Marine; Jacksonville, Nc *Jun 2006 – Jun 2010*

- Led missions as a Non-Commissioned Officer in an elite special operations unit, applying advanced risk assessment and operational planning.
- Specialized in reconnaissance, surveillance, and secure communications.
- Implemented an asset management system tracking $500,000+ in equipment globally.

EDUCATION | CERTIFICATIONS | TRAINING

- **2014 BACHELOR OF SCIENCE, UNIVERSITY OF OKLAHOMA.**
- 2015 JUNIOR PENETRATION TESTER (EJPT), E-LEARN SECURITY.
- 2016 WEB APPLICATION PENETRATION TESTER (EWPT), E-LEARN SECURITY.
- 2016 COMPUTER HACKING FORENSICS INVESTIGATOR, EC COUNCIL.
- 2018 ATTACKING AND DEFENDING MICROSOFT ACTIVE DIRECTORY, BLACK HAT 2018.
- 2019 WINDOWS AND LINUX BINARY EXPLOITATION, TROOPERS19.

SKILLS & INTERESTS

- **Vulnerability Research**: Coding in C/C++, taint analysis, Python POC exploit development, reverse engineering binaries, fuzzing.
- **Enterprise Security Leadership**: Leading blended security and engineering teams to deliver scalable, enterprise-wide platforms.
- **Threat Modeling & Risk Prioritization**: Identifying high-risk areas and implementing targeted solutions.
- **Strategic Security Operations**: Balancing security needs with cost and operational agility.
- **Offensive Security Engagements**: Red teaming, penetration testing, cloud security assessments, adversary simulation.
- **Collaboration**: Partnering with engineering teams to embed security in the product lifecycle.
- **Communication**: Translating complex topics for executives and non-technical audiences.
- **Penetration Testing**: Infrastructure, web app, cloud; OWASP ASVS familiarity; certified web app penetration tester.
- **Detection & Incident Response**: Threat, risk, and exploit analysis at scale; certified CHFI.