OWL Cyber Defense

Security Engineer

Department: Professional Services
Reports to: VP Professional Services

QUALIFICATIONS:

- BS degree in computer science, computer engineering, or related field

- 6 years of demonstrated experience in the field (candidates with at least 8 years of strong related work experience will also be considered without a degree)

- Current DoD Secret Clearance is required.

JOB KNOWLEDGE, SKILLS, ABILITIES AND COMPETENCIES:

- Knowledge of general security principles, protocols, and infrastructures

- Background in computer architecture, system internals and operating systems

- Interest in information security and cybersecurity

- Background or interest in research

- Analysis, testing, and debugging skills using tools like, ADB, gdb, Apktool, Wireshark, and tcpdump

- Experience with Android security mechanisms

- Familiarity with wireless/mobile technologies

- Knowledge of Android operating system/ frameworks

- Strong work ethic, self-starter, able to work independently, and willing to take on new challenges - to roll up your sleeves and do what you need to do in order to solve problems

- Desired skills include:
  - Knowledge of Linux/UNIX operating systems at all layers (boot, kernel space, user space).
  - Forensics and reverse engineering
  - ARM experience
  - High level of personal organization, persistence, and attention to detail
  - Certified Ethical Hacker (CEH) certification, or comparable certification

Job Summary

Owl Cyber Defense is looking for a highly skilled Security Engineer who has experience working in the full scope of mobile operating systems and applications security analysis. The individual will apply their expertise to perform penetration testing on hardened devices in our mobile device inspection lab.

Essential Duties and Responsibilities:

- Actively analyze security functions for design weaknesses, technical flaws and system vulnerabilities.

- Research new threats, attack vectors and risk and utilize their hacking skills on various mobile devices.

- Perform manual testing using various open source penetration testing tools.

- Have a strong work ethic, be a self-starter, able to work independently and willing to take on new challenges to roll up your sleeves and do what you need to do in order to solve problems.

- Operate with a high level of personal organization, persistence, communication skills, and be detail oriented.

- Document findings and creating recommendations for improved device security.