Software Security Automation Engineer

The Quality Engineering Team is looking to hire a Software Security Automation Engineer. As an SSAE at Scale Computing, your primary responsibility will be designing, developing, and maintaining core security and compliance automation solutions. This position will Develop solutions to identify, automate and test potential security vulnerabilities for all Scale Computing products. We believe in best-ever experiences from the inside out, so we're looking for an approachable, friendly candidate who loves security and hacking.

A great candidate will look like this:

- Has a passion for ensuring security best security practices are in place.
- Writes clean, highly readable, and testable code that rapidly identifies which product requirements have not been met
- Writes code that ensures product security requirements are being met.
- Experience running penetration testing against cloud services and local systems
- Enjoys troubleshooting and problem-solving
- Experience working with Product Management and Development Teams
- A team player who can work well within a team and collaborate cross-functionally, especially in a remote environment
- A motivated self-starter who thrives on prioritization and follow-through
- Passionately creative in mindset, and can adapt quickly to evolving business needs

Responsibilities

- Design and develop automated tests for both our appliance as well as our cloud services with a focus on security.
- Develop testing for a variety of situations, including usability, performance impact, error and bug finding, and regression testing
- Regularly run automated and manual penetration tests against both our appliance as well as our cloud services
- Identify, reproduce, and accurately document software and security defects
- Track known bugs, resolutions and software enhancements and ensure effective resolution and deployment of the Scale Computing product(s)
- Communicate frequently with developers on new and existing issues, including possible recommendations for resolution, improvements, and enhancements
- Self-education on Scale architecture and methodology
- Respond to external facing security concerns and questionnaires

Requirements

- A BS degree in a Computer Science, or equivalent work experience
- Minimum of 2 year of industry experience
- Minimum of 2 year with software security and penetration testing
- Experience with standard scripting languages, such as python, bash
- Experience using git
- Understanding of the Linux operating system and toolset
- Diverse exposure and understanding of a variety of operating systems, virtualization platforms, and understanding the interaction of the layers of technology (Network, storage, etc.)
- Organizational discipline and professional communication skills

Other useful skills/experience

- Technical knowledge and experience in the following: virtualization (mainline hypervisors), operating systems troubleshooting, IP networking, and storage technologies, both direct and NAS/SAN
- Experience with Ansible is preferred
- Exceptional communication skills, both verbal and written, as to communicate effectively, both up and down within the organization