Do you want your work to have real impact? Do you wish to directly contribute to the conception and implementation of highly innovative software solutions?

VMRay GmbH is an early stage information security company in Bochum, Germany. We develop innovative solutions and new technologies based on the latest academic research for automated malware analysis and threat detection. Our solutions are used by government and enterprise customers around the globe. We regularly present at the top international conferences such as RSA or Blackhat. To support our growth and expand our team we are hiring a

SOFTWARE ENGINEER – STATIC MALWARE ANALYSIS

Reference: **SMA-07/17**

· ·

We are a small, international team of 35 people. We offer modern and quiet workplaces instead of open-plan offices. Everybody arranges his working hours flexibly. At VMRay you will not be just a little cog in a big wheel. Instead, you will contribute to the conception and implementation of our products and solutions. Our technology and the problems we are solving with it are of high complexity. This is why our work is very challenging and it demands concentration and expertise. Every work day at VMRay is exciting and challenging due to a wide range of interesting customers and individual use cases.

We are not just sitting in a professional Ivory Tower but meet regularly with IT security experts from all over the world. We present our products at international conferences and give speeches at invite-only hacker workshops.

Please send your application documents (including reference number and salary expectations) as pdf version by email only to jobs@vmray.com!

We offer flexible working arrangements for remote work.

RESPONSIBILITIES

* Design and implement static analysis engine for our malware analysis framework
* Write parsers for various document and executable formats (PDF, Office, PE, etc.)
* Identify meaningful distinct characteristics of malicious documents (detect shellcode, malformed source code, etc.)
* Create scoring system to statically assess file maliciousness

SKILLS & REQUIREMENTS

* Strong interest in malware analysis
* Ability to efficiently read up on file formats and state-of-the-art exploitation techniques
* Proficient with Python programming or at least one similar high-level programming language