VMRay
Agentless Threat Detection

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, above all in North America. 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

THREAT RESEARCHER

Reference: **TR-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

- Collaborate with development team and provide detailed malware analysis information to improve product quality
- Write blog posts, articles and hold technical presentations at various conferences
- Obtain an in-depth understanding of the current malware landscape (today's threats, actors, techniques, etc.)
- Actively follow current discussions and trends on relevant social media sources

SKILLS & REQUIREMENTS

- Proven knowledge of malware landscape (tools, strategies, etc.)
- Hands-on experience with relevant reverse engineering tools (Ollydbg, IDA Pro, etc.)
- Proven experience in defeating both established and sophisticated anti-analysis techniques
- Strong knowledge of x86 assembly programming
- In-depth understanding of the Windows API and internals relevant to malware analysis
- Fluent in verbal and written English