NVISO
SECURITY * RESEARCH * RISK

Reverse Engineering and Malware Analyst

Our profile

NVISO is a pure-play cyber-security consulting firm: our team is composed of security professionals that each have their specific field of expertise, ranging from Information Security Governance, Risk & Compliance to Incident Response, Penetration Testing, Software Security and Training & Awareness. This fantastic blend of skills enables us to help organizations prevent, detect and respond to complex security challenges.

NVISO is also known as a Belgian Cyber Security start-up: through our active investment in Research & Development and partnerships with Belgian academic players, we are investigating emerging threats and trends, refining our techniques and developing innovative products that make NVISO a unique player in the market.

Our team is built on the values of Entrepreneurship, Commitment, Integrity, Client-Orientation and Respect, which neatly ties into our mission to be an innovative, trusted and respected security partner for our clients. And we are looking for new colleagues that are as enthusiastic about these values as we are! So come and join us!

Job description

We are looking for a professional with strong programming skills, excellent technical skills to research the latest malware families, good malware distribution techniques, able to conduct independent research and to perform detailed malware analysis, analyse cyber threat data, and create intelligence reports.

As reverse engineering and malware analyst you will dissect attacker tools and backdoors. You will also help to develop innovative tools and automate malware analysis.

Your profile

- Master degree or other higher education in a technical discipline;
- Advanced experience in computer engineering or a related field with in-depth knowledge of software reverse engineering and/or software development;
- Knowledge of programming and scripting languages: Assembly x86/x64, C, C++, Python, JavaScript, Java, PHP, and HTML;
- Experience using static analysis tools such as IDA Pro, OllyDbg and dynamic analysis tools including debuggers;
- Ability to analyse obfuscated code;
- Proficiency in Windows OS Internals and APIs;
- Familiarity with vulnerability exploitation and identification is a plus;
- Preferred but not mandatory that applicant is eligible to receive a BE/EU/NATO clearance;
- Experience with computer forensics and malware analysis tools;
- Knowledge of malware packers, obfuscation techniques, and exploit kits;

- Familiarity with mitigation strategies such as Snort and YARA signatures;
- Strong leadership, interpersonal and verbal/written communications skills that enable the ability to work effectively in a collaborative team environment;
- Excellent Dutch, French and English communication skills, both verbal and written;
- Produces clearly written and concise research reports;
- Ability to prepare and present research findings in both client and public settings;
- Excellent customer service and communication skills as well as the ability to prioritize and meet deadlines;
- Team player who works well under pressure;
- Candidates must recognize and deal appropriately with confidential and sensitive information.

Our offer

- Working and learning from the best people in the cyber security industry in Belgium. We have two SANS Instructors working at NVISO, our staff has presented at popular hacking conferences (BlackHat, BruCON, etc) and all of our technical staff must acquire deep technical security certifications (GSE, GXPN, GREM, GCFA, OSCP, etc);
- Your personal 5+5 learning budget (5.000 EUR and 5 days) every year. Most of our staff either follow a SANS training each year, or spent their budget on traveling to conferences like Blackhat/Defcon or RSA;
- Contribute to initiatives like the Cyber Security Challenge Belgium;
- An attractive and market-aligned reward package including company car and health insurance.

Interested?
Then send your CV and a motivation letter to **jobs@nviso.be**!