Senior Incident Response Consultant

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

To strengthen our Forensic team, we are seeking for a Senior Incident Response Consultants with strong technical skills and able to work in teams, to communicate with clients and to deliver high-quality analysis and deliverables.

The candidate will be responsible of:

- Conducting analysis on end-user and server based systems in large and small scale environments;
- Log analysis of a multitude of different sources including host and network devices;
- Malware analysis;
- Analysing and correlating log data, malicious software behaviour, system state changes, and other information across multiple systems to forensically reconstruct malicious activity and impacts;
- Networking environments, architecture and information security;
- Network packet capture and analysis;
- Recovering deleted files, reconstructing Internet history, using GREP search techniques, analysing metadata, carving unallocated clusters, analysing registry files, imaging files from servers and RAID arrays, and similar forensic techniques;
- Researching computer processes, system state, and connections from running systems during incident response;
- Building, maintaining, and upgrading computer forensics hardware and software;
- Experience as an IT security administrator is preferred;
- Experience in computer programming is preferred.

Your profile

Forensics:

- Excellent working knowledge of EnCase, as well as open source alternatives;
- Experience with scripting in Perl/Python/Ruby;
- Experience with both desktop-based and server-based forensics;
- Experience with compromises involving web applications.

Penetration Testing:

- Excellent working knowledge of computer networks and their vulnerabilities;
- Excellent working knowledge of layer-two networking issues;
- Excellent operating system knowledge in Windows-based and Unix-based systems;
- Demonstrable experience with a wide range of different attack tools;
- Application testing skills.

Other Requirements:

- 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**!