JOB DESCRIPTION

CYBER SECURITY ENGINEER

RIELA HQ: DOUGLAS, ISLE OF MAN

The role in a nutshell

This is not your standard Cyber Security Engineer opportunity. We work at the cutting edge of cyber security, providing pro-active and holistic cyber security services to our clients to ensure that their businesses are secure. Not only do we provide CISO and cyber security consulting services, Riela Cyber also provides state-of-the-art monitoring solutions, follows industry best practice when it comes to forensic investigation and incident response and assists its clients with comprehensive security audits and pen tests. As part of our cyber security team, you will take on a broad role, as you will not only work on evolving our product offering but you will also work closely with our clients to ensure that they are protected.

What would I be doing?

In this position you will play a very important role for us. The demand for the role has been created by our growth, and you will be a key enabler for the continued expansion of our business.

In this role you will have both broad and deep responsibilities across building and delivering our services to our clients, including:

- Monitor and investigate the company's own and its client computer systems and digital assets for cyber-attacks, incidents and breaches.
- Develop client and management reports from investigation, monitoring and response efforts.
- Implement strategies for mitigating damage and preventing future cyber-attacks, incidents, and breaches.
- Assist with auditing and measurement of security controls internally and for our clients.
- Identify risk within internal, external and cloud-based infrastructures.
- Automate / improve current processes and repetitive daily tasks.
- Perform cyber defence incident triage, including determining scope, urgency, and potential impact, identifying the specific vulnerabilities. Make recommendations that enable expeditious remediation. Design, review applications and architecture adhering to best practises and security standards.
- Conduct both local and remote penetration testing designed to emulate current threat models to execute an assessment of our clients' defensive security posture.
- Execute high-risk web assessments, non-notice penetration testing of assets, on-demand testing of network devices, and other activity required to assess the defensive posture of the targeted network.
- Execute research to develop payloads used during penetration testing and/or phishing that emulates the current threats to our client networks, to test whether defensive devices will detect this activity proactively.
- Develop and execute security strategies with our clients to improve their security posture, either in the role of a vCISO or security consultant.
- Perform web, mobile and cloud penetration tests and assessments
- Perform vulnerability risk assessments on our clients' internal and external facing environments

You will directly report to the Director of cyber security. You will also work very closely with our infrastructure and client relationship teams.

What skills and experience are you looking for?

We are looking for a Cyber Security Engineer with extensive experience in a broad spectrum of cyber security and interpersonal skills.

You will have the opportunity to add value to our clients by directly liaising with them to build their security posture and develop a holistic security strategy. We focus on long-term partnerships with our clients which allows you to utilize your extensive skillset to provide them with the best solutions to meet their objectives.

You will have an an excellent understanding of offensive and defensive security frameworks, including experience in public speaking engagements, providing expert opinions, and conducting structured training courses internally as well as to our clients, both at a technical and at a board level.

We are looking for someone with good knowledge in most of the following areas:

- <u>Industry Standards:</u> NIST, ISO, PCI, CIS,
- <u>Security Frameworks:</u> MITREATT&CK, Cyber Kill Chain
- <u>Security Applications:</u> Nessus, Kali Linux, Metasploit, Cobalt Strike
- <u>Web Application Tools:</u> BurpSuite
- <u>Cloud Applications:</u> AWS, Azure
- <u>Development Languages:</u> Python, Ruby, Java, Powershell

Qualifications:

- <u>Essential:</u> OSCP, SEPP

Tell me about you?

Riela is a growing company with an entrepreneurial spirit. Our heritage is in e-gaming and Yacht management sectors, both for Ultra High Net Worth Individuals (UHNWI) and SME's. As the landscape is changing, we have evolved with it but we have never lost sight of our heritage in building long-term trusted partnerships with our clients. Since the early days of Riela we have expanded our offering to help both individuals and companies manage high value and digital assets. Our clients are global and so is our mindset. We combine state-of-the-art technology with our people's skills to provide more efficient services to our clients across the world.

Our core values of Integrity and Support underpin everything we do, how we act with our clients and how we act with each other. You can be confident when joining Riela you will be a part of team that will work with you to achieve our shared goals.

We are on an exciting journey, evolving our culture to represent the changing products, services and people that make up the Riela Group. It is a great time to join and play your part in this trip.

Riela: Everyone is welcome.

At Riela we believe that we will achieve our best by recognizing the value that every individual will bring to work. We are committed to inclusion across age, gender, identity, race and religion. We are committed to creating an environment where everyone is welcome.

Salary and benefits

We offer a competitive salary and fantastic benefits including a pension scheme with a 9.5% company contribution, non-contributory, health cover and free parking at our office.

What happens next?

If the above is of interest, we like to keep it simple, drop us a copy of your CV to hr@riela-group.com. If it looks like a good fit, the next stage will be initial telephone interview with our HR team to get to know you a bit better, the next and final stage will be structured interview with one of our directors and someone from the tech team.