JOB SPEC

Senior Cyber Security Analyst

About the job:

We are looking to recruit a Seniro Cyber Security Analyst to join our IT function in Northampton. This is a full time role, working 35 hours per week Monday to Friday, based in our head office in Northampton, with some flexibility to work from home.

The Senior Cyber Security Analyst is required to undertake a range of tasks supporting the Cyber Security Manager and iPSL key business objectives as directed within the Cyber Security environment. The role will be responsible for investigating and remediation of all Cyber Security related incidents within the company, for ensuring vulnerabilities are managed and remediated and for helping to ensure the business is aligned to recognised Cyber best practices and for maintaining appetite within the security risk framework, supporting the delivery of internal and external cyber security service operations and for assisting in the monitoring and evaluating of security service improvements to the MSSP/ SOC.

Some of your key activities will include:

- Proactively search for active intrusions in the IPSL environment, recognising potential, successful, and unsuccessful intrusion attempts and compromises through reviews and analysis of relevant event detail and summary information
- Conducting holistic, investigative analysis and rating the risk associated with observed activity
- Review investigation escalations from Cyber Analysts to ensure accurate analysis and provide advice/mentorship
- Refine and develop dashboards, queries and reports to continuously improve security situational awareness and provide monthly reports to appropriate senior managers detailing the status of the iPSL Threat landscape.
- Provide assistance with contract queries and negotiation regarding the MSSP / Managed SOC.
- Responsible for gathering key stakeholders on a regular basis to define improvements and provide updates on the status of security tooling deployed in IPSL
- Act as SME for ensuring strong and effective security controls are in place to detect and mitigate risks across all on-prem and Cloud environments to meet business objectives and regulatory requirements.
- Responsible for improving and automating existing activities by leveraging automation and scripting with a view to increasing reliability and reducing time of execution, colleague dependencies and vendor lock-in.
- Responsible for supporting the delivery of Information Security policy, standards and guidelines documentation across the organisation and client base
- Assist with the delivery of the Information Security Awareness programme across the organisation
- Promote DevSecOps, leading by example to change existing systems and practices for the better, allowing all functions to do more with existing resources.
- Provide consultative Cyber Security support to the rest of the business (I.E. providing security expertise/guidance and sign off on relevant changes or unique requests/actions not covered by policy).

- Provide mentorship and point of escalation for junior members of the team.
- Assist with the identification of Cyber Security Risks in conjunction with both Cyber Risk and the business, assisting to qualify and support the risk owner in the development of appropriate controls by way of mitigation
- Responsible for aiding in the detection, monitoring, analysis and remediation of vulnerabilities across IPSL's environments
- Undertake activities as directed to assure the operational effectiveness of controls that mitigate or otherwise manage Information Security risk within tolerance
- Contribute to the production of accurate and timely management information as requested by IS management.
- Identify opportunities to improve service, quality and efficiency.
- Any other reasonable task within the scope of this level

To be successful in the role you will need to have:

Essential

- Experience of working in Information Security or Cyber Security in a relevant role, e.g SOC Analyst, Security Engineer, System administrator, Consultant, Architect, Analyst.
- Extensive experience delivering and supporting technical solutions at an Enterprise level, with a track record of instigating and implementing change.
- Previous experience with application security , DevSecOps or working alongside developers bringing culture, automation, lean, measurement, everything-as-code and sharing into Information Security at the same time as embedding security into DevOps tooling and processes.
- Confident and able to build good working relationships with direct team and internal customers.
- Commitment to deliver and maintain high levels of customer satisfaction.
- Confident to provide information and recommendations to key stakeholders on security issues.
- Effectively prioritises tasks to ensure delivery meets time critical deadlines.
- Good written and verbal communication skills.
- Experience working with typical security toolsets and tuning rules where appropriate i.e. SIEM, IDS.
- Proven experience conducting Cyber Security investigations in On-Prem or Cloud environments
- General understanding of IT Security principles, standards and regulations (e.g. ISO 27001, NIST, GDPR (DPA).
- CISSP
- Azure / AWS/ GCP qualification
- Security+ / CySA+

Desirable

- Experience in a regulated industry, e.g., financial services.
- Experience of IPSL systems
- OSCP / CREST CRT / SANS GIAC 503 or 504

Compensation & Benefits

If you have the knowledge and skills detailed above, then here are just some of the benefits available to you:

- Competitive salary, **£29,500 to £46,500** p.a. (depending on experience)
- £4,100 p.a. Car Allowance
- Generous holiday allowance – 25 days per year, plus 8 Bank Holidays
- Private family healthcare
- Funded healthcare cash plan
- Matched company pension contribution up to 7% and many more benefits!

An organisation is only ever as good as its people. Here at iPSL, our people power our vision and we go to great efforts to ensure we engage and invest in our people at every opportunity. You can find out more about what's on offer when you work at iPSL via our website.

How to Apply

Please apply **via this link** and make sure you enter the vacancy reference **539555** in your application.

If you are successful, a member of our team will contact you to arrange an interview – this could be either via telephone, video conference or in person. You can find out more about our recruitment process on our website.

PLEASE NOTE: Interview dates will be during w/c 15th and 22nd August

Due to the volume of applications we receive, we are not always able to respond directly. If you have not been contacted by 30th August 2022 we regret that you have not been successful in securing a position at the next stage of the process.