SECURITY OPERATIONS ANALYST

CHELTENHAM

PERMANENT, FULL TIME (FLEXIBLE)

At iPipeline, we pride ourselves on our culture. We believe in an enthusiastic atmosphere, encourage innovation, depend on creativity, and strive for success. We value our employees and understand that our continued success as a company relies heavily on the success of every individual. Our employees describe iPipeline offices as fun, energetic, 'can do', professional environments.

We empower our people and provide them with the opportunity to pursue personal growth and career aspirations. We work hard and play hard. We celebrate success.

As the market leader in our industry, we deliver ground-breaking and award-winning technology to the financial services industry. Working at iPipeline allows you to play a huge part in making it easier for our customers to protect and secure the financial futures of consumers' families.

YOU CAN ENJOY:

- Innovative, inclusive and focused environment
- Flexible working
- Work/life balance
- New, contemporary, open-plan office space
- Company matched pension benefits
- Generous Life and Critical Illness Cover
- Perkbox membership (discounts and freebies)
- Competitive holiday allowance
- Well stocked kitchen of free soft drinks, tea, coffee and fruit
- An annual wellness allowance to keep you happy and healthy

PURPOSE OF THE ROLE:

The Security Operations Analyst is responsible for the operation and configuration of security tools that identify and detect potentially malicious activity. This is a technical position that requires experience in operation of various security tools. The position will act as a security incident analyst or manager as part of the Computer Security Incident Response Team (CSIRT). The position will work with MDR as well as co-managed SIEM solution providers to continually enhance our detection and response capabilities.

RESPONSIBILITIES:

- Manage and maintain Critical Security Systems and Controls
- Ensure effective security monitoring, alerting, and reporting systems are in place
- Monitor for and investigate suspicious and potentially malicious activity
- Tune security controls to improve detection
- Effectively manage any security-related incidents
- Investigate, document, and report on information security issues and emerging trends
- Analyse and respond to previously undisclosed software and hardware vulnerabilities
- Identity and Access Management responsibilities
- Keep abreast of security technology and developments within the cybersecurity field and their impacts on and potential benefits to iPipeline
- Manage and develop relationships with counterpart security professionals at iPipeline, and other stakeholders
- Operation of the iPipeline security awareness program including training and phishing tests
- Attend appropriate training opportunities to keep up with industry trends and career development
- On call duty for responding to security incidents

SKILLS:

REQUIRED

- Knowledge and experience in cloud platform security (AWS)
- Recognized Security Industry certification e.g. SANS, CISSP, CISA, CISM or equivalent education
- Knowledge of technical security controls, their design, implementation, and operation
- Working knowledge IP and relevant Internet technologies
- Attack principles and the cyber kill chain
- Keen interest in security, investigating, concluding investigations based upon evidence
- Previous experience with EDR, SIEM, Vulnerability Management, IDS/IPS

DESIRABLE

- Scripting and programming skills
- Prior SOC experience highly desirable
- Automation of daily security operations
- Creation of security playbooks or runbooks
- Experience with Okta or other IDP
- Experience with threat hunting and forensics

PERSONAL QUALITIES:

- Passionate about technology and information security
- Ambition for continuous learning
- Analytical/detail oriented
- Self-motivated

- Desire to understand how things work
- Ability to clearly articulate security issues, risks, and best practice to all levels of iPipeline staff
- Excellent at cross-team working

DON'T HAVE EVERYTHING WE'VE ASKED FOR?

Don't worry.

You might not have everything listed above but you might have some valuable transferable skills and experience.

You might be returning from a career break or feel you have taken a wrong turn in your career.

At iPipeline, it's about you and what makes you tick, not ticking every box.

To apply please email cheltenham.recruitment@ipipeline.com with your CV and covering note (don't forget to include those transferable skills).

For information on how we store applicant information, please see our Job Application Privacy Policy.