

JOB DESCRIPTION

Job Title:	Junior Security Analyst
Department:	IT
Location:	Theale
Reporting to:	IT Director

About Clearswift

Clearswift is trusted by organizations globally to protect their critical information, giving them the freedom to securely collaborate and drive business growth. Our unique technology supports a straightforward and 'adaptive' data loss prevention solution, avoiding the risk of business interruption and enabling organizations' to have 100% visibility of their critical information 100% of the time.

Clearswift operates world-wide, having regional headquarters in Europe, Asia Pacific and the United States. Clearswift has a partner network of more than 900 resellers across the globe.

More information is available at www.clearswift.com

Clearswift Values

Show *passion* in what we do, drive for *innovation* in everything we do and continuously *collaborate* to make a difference.

The Role

The Junior Security Analyst is responsible for the day to day administration of the Information Security Management System (ISMS) in addition to the administration and maintenance of enterprise systems. Job responsibilities will also include auditing and reporting of systems and applications

Key Responsibilities

- Actively monitor and support internal and external systems infrastructure systems (Incident & Problem Management), liaising with colleagues in regional location as necessary
- Compile comprehensive audit reports identifying potential risks / threats
- Report on KPIs in relation to compliance and effectiveness of the information security controls and ensure the reporting to key stakeholders
- Advise and support the IT Security Manager with defining specific information security controls and policies
- Lead the internal information security awareness program and ensure all staff achieve annual accreditation
- Carry out security assessments in relation to projects and change management
- Support the IT Security Manager in developing an IT security assurance program
- Maintain the threat and information risk register and recommend the appropriate remediation
- Develop general and detailed documentation describing system specifications and operating instructions
- Ensure infrastructure, applications and data security/privacy controls are maintained in compliance with corporate and regulatory policies
- Participate as a member of the Service Desk support team resolving client side issues as and when needed
- Develop appropriate project related documentation/business cases. Implement projects in accordance with policy ensuring the identified goals and objectives are delivered on time and within budget
- Procure IT related resources in line with company policy and ensure accurate record of assets is maintained
- Support business continuity processes (backups, replication etc) through continued documenting and testing of infrastructure environment
- Liaising & maintain appropriate relationships with third party vendors
- Help staff with use of the company systems, providing training where necessary
- Participate in out of hours support coverage (1 week a month)

Skills Profile

- A strong understanding of security & networking technologies
- Strong analytical and problem-solving skills
- Team player
- Excellent communication and interpersonal skills
- Ability to cope and work under pressure
- Innovative, flexible and open approach
- A results oriented individual who thrives working in a fast-paced environment
- Self-motivated with the ability to prioritize, meet deadlines, and manage changing priorities

Technical Profile

Required Knowledge and Experience

- 3+ years' experience implementing and managing core Microsoft stack (MCSE equivalent certification)
- Automation tools and applications
- Various scripting technologies
- Desktop application deployment
- 2+ years' experience administering and support virtualization platforms (VMWare AND Hyper-V)
- 1+ years' experience implementing and managing with Linux operating systems
- Experience managing cloud solutions (IaaS, Azure, AWS)
- Experience managing data centre technologies (SAN's, Switches, VLANs, Routers, Servers, Firewalls)
- Able to demonstrate an understanding of ISO27001:2 and information security best practices (identity management, intrusion detection/prevention)
- Able to demonstrate a solid understanding of ITIL principles
- Experience managing Firewalls and other security related devices.
- Experience preparing project documentation and managing projects through to completion

Desirable Knowledge and Experience

- CompTIA+ Security or equivalent certification
- Certified networking credential (CCNA or equivalent)
- Endpoint management solutions
- Virus protection & other prevention solutions
- Mobile Device Management

Other

- Participate in out of hours support coverage
- Ability to travel Globally