ENCOMPASS

JOB DESCRIPTION

Job Title:	Platform Security Specialist
Location:	Chiswick, London
Reporting to:	Manager, Platform Engineering Infrastructure
Hours of work:	Full time, 37.5 hours per week (Monday – Friday)

Main Purpose:

This is an opportunity for an information security specialist to aid our upcoming TPN IT security audit accreditation. We are seeking an expert in this field to advise on the best means to implement appropriate security measures to achieve accreditation & establish processes to maintain our ongoing conformance. This is a hands-on role to implement the recommended security measures & tools in-line with our existing business practices and to document these changes. The role will also be responsible for defining and implementing additional processes for regular reviews of our IT security robustness to ensure continued compliance. The role will report into the Platform Engineering team who maintain the systems, and will carry out the ongoing reviews so there is a requirement to ensure the team is suitable upskilled to manage the tools and processes implemented in the long term.

Principal Responsibilities:

- Provide subject matter expert capabilities on IT security for production systems
- Identify areas of existing networks and systems where changes are needed to meet industry best practice for IT security.
- Specify and implement IT security tools on production systems to achieve TPN industry security accreditation.
- Develop IT security policies aligned with industry best practice to ensure compliance with future security audits.
- Define and implement regular review processes for IT security to ensure level of IT security is maintained long-term.
- Configure firewalls, IPS/IDS systems, VPNs and switches to ensure network security.
- Advise on/implement penetration testing tools for production network.
- Deploy syslog/SIEM tools to provide logging and audit trail of activity on networks/systems.
- Define and apply Microsoft Windows Active Directory and Group Policy configurations to implement IT security policies.
- Implement OS/Software patch management tools and procedures where appropriate for Windows & Linux systems as well as network/firewall hardware.
- Configure workstation security tools including anti-virus/anti-malware and URL filtering to maximise security without degrading business effectiveness.
- Liaise with user group managers to explain changes and ensure smooth implementation.
- Train Platform Engineering team members where needed to review configurations/logs and security tool data to identify and understand risks and potential security breaches.
- Document IT security systems implemented to enable ongoing support/maintenance.
- Report progress and blockers to project/programme managers.

Experience/Knowledge:

- 5+ years of network security experience
- Palo Alto firewall configuration
- Cisco ASA/ISR firewall configuration
- IPS/IDS technology
- Syslog/SIEM tools
- Cisco L3 switches (Nexus & Catalyst) & ACLs
- Microsoft Windows Active Directory & Group Policy
- Linux Administration/hardening (CentOS preferred)
- Site-to-site and user access VPNs
- Anti-virus/Anti-malware
- URL filtering (Cisco Umbrella)
- OS/Software patch management and deployment (WSUS etc)
- Penetration testing solutions
- Large scale production networks with multiple workflows and complex connectivity for multiple clients
- Experience in documenting IT systems for 2nd/3rd line teams and transferring skills/knowledge to peers
- Well experienced investigating challenging problems in complex E2E systems, with excellent analytical & troubleshooting skills
- Experience managing relationships with key internal stakeholders and project managers
- Educated to Degree level in an IT/Engineering related discipline, or equivalent work-based experience
- Broadcast/Media IT system experience would be beneficial

Personal Skills:

- Highly motivated self-starter, able to learn quickly and work independently
- Collaborative team player with a strong ethos of knowledge sharing
- Honest and accountable, with a strong sense of ownership
- Excellent interpersonal skills and ability to communicate effectively at all levels, whether face-to-face, verbally or in writing
- Logical, thorough approach to tasks with appropriate understanding and management of risk of changes to live systems
- Ability to present new operating processes/protocols and obtain buy-in from user groups
- Thrives in a fast-paced, sometimes high pressure, environment, reacting quickly and calmly to evolving tasks and competing priorities
- Flexible, willingness to work out of hours when required to get the job done