IT Security Analyst

Job purpose:

Monitor security logs across the Law Society. Assist the IT Security Manager to investigate security breaches and other cyber security incidents. Install effective security measures and operate software to protect systems and information infrastructure, including firewalls and data encryptions.

Key Accountabilities:

- Effectively monitor the Law Society's estate computer networks for security issues
- Ability to learn and apply new security concepts
- Investigate security breaches and other cyber security incidents, resolving them efficiently
- Install security measures and operate software to protect systems and information infrastructure, including firewalls and data encryption programs
- Clearly document security breaches and assess the damage they cause, whilst also making well considered recommendations to avoid similar security breaches
- Collaborate well with the IT Security Manager to perform tests and uncover network vulnerabilities
- Assist with resolving detected vulnerabilities to maintain a high-security standard
- Research security enhancements and make well considered and informed recommendations to IT Security Manager
- Examine security systems and web applications
- Monitoring security access across the Law Society
- Assist with conducting security assessments through vulnerability testing and risk analysis within good time and to a high standard
- Assist with performing both internal and external security audits
- Analyse security logs from various system for breaches and make recommendations as appropriate
- Assist in verifying the security of third-party vendors and collaborating with them to fulfill security requirements.
- Review daily security logs for abnormal events and escalate them to the IT Security teams in a timely manner.

- Conduct technical vulnerability assessments and regular penetration testing of IT systems and processes to identify potential vulnerabilities and provide recommendations for risk mitigation.

Knowledge, skills and experience	**Planning & Organising**
Essential: • BSc in Cyber Security, Computer Science, or equivalent practical experience. • Demonstrable technical knowledge of hybrid estate • Relevant experience of reviewing technical security events • Skilled in implementing a robust and trustworthy security configuration for various devices, ensuring that all security protocols are effectively set up to protect against unauthorized access and potential threats. • Substantial experience of testing and reviewing security solutions • Practical experience of effectively managing cyber incidents • Strong reasoning and advisory skills, with the ability to effectively engage with and influence senior management • Able to communicate confidently and effectively with staff at all levels in the organisation • Able to collaborate well with third parties to understand critical security bottlenecks • Strong knowledge of Microsoft Defender and network architecture • Substantial experience in a Security Operations Centre (SoC) , Network Operations Centre (NoC) • Strong understanding of Incident Response processes and methodologies and experience with MITRE ATT&CK framework to map and analyse threats. • Knowledge of Endpoint Detection and Response (EDR) platforms • Familiarity with threat hunting techniques and processes	Essential: • Able to plan, organise and prioritise work items as needs arise and maintain a positive can-do approach

• Certifications such as GSEC, CISSP, OSCP, MaD are preferred. Certified Soc Analyst (CISA) or CompTIA Cybersecurity Analyst (CSA+), or Cisco Certified Network Associate • Familiarity with NIST, ISO 27001, and CIS Controls. • Experience in monitoring, incident response, and vulnerability management. CISA, SSCP, or CompTIA Sec+ certification is a plus. • Proficient with SIEM, IDS/IPS, vulnerability scanners, and Azure security tools. • Knowledge of ITIL processes for effective IT team integration. • Strong team collaboration and ability to effectively communicate security matters to non-technical audiences to support wider employee engagement • • Able to produce reliable and quality work on time during periods of pressure • Ability to effectively manage wellbeing being during busy and pressured moments at work, with support from the Law Society as appropriate • A proactive approach to supporting a respectful and welcoming environment at the Law Society • Assist with building and continually improving IT security for TLS and its members • Assist with managing and developing the Law Society's approach and understanding of IT security • Ability to resolve conflict and to deal with competing priorities • Support the execution of the Cyber Strategic Plan while continuously seeking innovative methods to enhance the cyber security function, reduce risk across the organisation, and improve customer and colleague experiences. • Oversee and manage cyber security governance controls in line with Cyber Assurance Framework, including tracking performance through KPIs and SLAs, supporting vulnerability, management activities and providing relevant management information as needed.	

Desirable: • Scripting and automation • Digital forensics • PCI • Network Analysis • SDLC	**Organisation Chart**

Location 113 Chancery Lane, London, with hybrid working	