SECURITY ENGINEER

Key Responsibilities

- Improve the security of the production IT infrastructure estate
- Design, implement and monitor IT security controls that effectively address identified security risks and compliance requirements
- Review changes to the IT infrastructure estate for any potential security impacts
- Vulnerability Management – maintain regular scans, interpret results, identify asset owners, track remediation activities and report on the agreed SLAs.
- Security Controls Administration – maintain availability and functionality of all security controls; implement new and advanced features where available; write technical documentation and manage changes
- SIEM Maintenance & Content – maintain availability of the underlying infrastructure, develop new alerts, field parsers, models and automated playbooks, and integrate new log sources where appropriate
- Threat Intelligence & Threat Hunting – provide, develop and integrate external threat intelligence data into the team's detection capabilities; perform proactive threat hunts based on working hypotheses, and implement subsequent SIEM alerts where required
- Insider Threat – maintain and develop the Data Loss Prevention policies in line with the company's data classification requirements and implement exceptions for business approved procedures where required. Improve the detection and response capabilities of the remaining security controls with a focus on insider threat.
- Focus on secure configuration, best practice processes, automation, and delivery of industry leading security tools within the IT infrastructure estate

Skills & Experience

Essential

- At least 2 years SOC or security experience is required
- ISO 27001/2, NIST, PCI DSS, SOX, ITGC, or other security frameworks
- Deep familiarity with one or more SIEM tools is required
- A strong understanding of technical IT concepts is required, including: Windows and Linux operating systems and system administration; networking, including TCP/IP and other common protocols
- Command line interfaces and scripting

- Understand the role, benefits/downsides, and standard use cases of technical security products, such as firewalls, antivirus, web proxies, SIEM, IDS/IPS, DLP, and EDR
- Experience with vulnerability scanning and penetration testing tools and techniques (ie: Nessus)
- Strong ability to focus and complete detailed tasks with high degree of accuracy
- Significant experience in monitoring and managing IT security systems (AV/anti-malware/two factor auth/phishing threat management
- Proficient with MS Office for general collaboration, communication, and reporting
- Firewall – FortiGate; PFsense or equivalent technologies
- SIEM & SOAR: detection engineering and response automation

Desirable

- Purple Team & Scenario Exercises – regularly test the team's detection capabilities, develop scenario-based training, and organized purple team exercises, both in house and with third party providers
- Experience with network forensic tools, such as network sniffers and protocol analysers
- Desirable certifications include: CISSP, CEH, CREST, OSCP Security+, Network+, CySA+
- Vendor certifications for Microsoft, Linux, cloud, networking or security products