L&Q Group

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Role title | | Graduate Infosec Analyst | | | | | | | | | Date | | 13/09/21 | | |
| Reports to Title | | Infosec SOC Lead/Manager | | | | | | | | | Version | | FINAL | | |
| DBS Disclosure Required: | | Yes |  | No | X | Standard | |  | Enhanced | |  | Enhanced  + | |  | |
| Responsibility for End Results | | | | | | | | | | | | | | | |
| Support infosec security operations team in proactive monitoring, reviewing and investigation and report Technology Security incidents. This role will support the infosec SOC analysts in assessments and improvements to technology security monitoring, processes and communications. They will need to work closely with Technology and Digital Teams ensuring network, applications and systems access monitoring are reviewed and analysed. | | | | | | | | | | | | | | | |
| *Key Responsibilities / Deliverables:* | | | | | | | | | | | | | | | |
| Main Accountabilities: List the major activities or functions necessary to achieve the job’s end results. The percentage of time spent on each of these should add up to 100%. | | | | | | | | | | | | | | *Time (%)* | |
| 1. Customer service/ values  • Assist in the wider information security program with a particular focus on vulnerability management, monitoring, log and report analysis, risk mitigation, and controls. | | | | | | | | | | | | | | 10 | |
| 2. Strategy/ achieving objectives   * Working with and assisting the infosec team to support the development and delivery of information security controls, providing assurance that controls are maintained. * Working with and assisting the infosec security operations team to support delivery and maturity of Information Security function aligned to Infosec roadmap and corporate values * Additional Duties as required by management; this may include travel between L&Q sites and working remotely | | | | | | | | | | | | | | 10 | |
| 3. Working with others – internal  • Integrate and share information with other analysts and other teams. Work collaboratively with information security team, technology, and document and report on information security issues and emerging trends | | | | | | | | | | | | | | 20 | |
| 4. Working with others – external   * Work collaboratively with partners as required, including external suppliers | | | | | | | | | | | | | | 5 | |
| 5. Budgetary responsibility  • Adopt responsibility for the creation of value, and cost efficiency in all aspects of day-to-day work | | | | | | | | | | | | | | N/A | |
| 6. Compliance  • Keep abreast and research information security trends, new external risks, threats and vulnerabilities. | | | | | | | | | | | | | | 10 | |
| 7. Records and systems  • Support and participate in helping the team resolve major and security incidents, post implementation reviews and problem reviews to assist with the identification, review and analysis of security incidents or threats to service. Would also be involved in assisting with performing Pen Testing and Vulnerability scanning.   * Support and help the infosec team in capturing evidence and documentation aligned to infosec team and technology process and best practice * Support continuous monitoring of company infrastructure to identify security incidents and proactively report and manage these. | | | | | | | | | | | | | | 35 | |
| 8. Risks  • Support and help capture new and existing risks, vulnerabilities and threats aligned to information security risk management. Also would assist in checking security protection is up to date to help to minimise risk by helping perform regular spot checks. | | | | | | | | | | | | | | 10 | |
| Financial Responsibility: Enter below any revenue, operating or capital budgets for which the role is accountable. | | | | | | | | | | | | | | | |
| N/A | | | | | | | | | | | | | | | |
| People Responsibility:  Indicate below the number of employees for which the role has supervisory / management responsibility. If the number varies, indicate an average or a range. | | | | | | | | | | | | | | | |
|  | | | | | | | | | | *Direct Reports* | | | *Indirect Reports* | | |
| Total Employees | | | | | | | | | | 0 | | | 0 | | |
| Please list below any outsourced service providers that are managed by the role (e.g. payroll), or any functional / project management responsibilities. | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | |
| Technical Knowledge/Skills | | | | | | | | | | | | | | | |
| List of technical knowledge/ skills required to successfully perform the job role; including professional qualifications | | | | | | | | | | | | | |
| * Foundation knowledge of various security methodologies, processes, and technical security solutions (firewall and intrusion detection systems) | | | | | | * Foundation level understanding of information security best practice. | | | | | | | |
| * Foundation Knowledge of Security solutions such as Antivirus/Malware, routers, firewalls, cloud, IDS, Full Packet Capture and Host/Network Threat Analysis. | | | | | | * Foundation understanding of identification of cyber threats, malware, viruses and system breach indicators. | | | | | | | |
| * Foundation knowledge and understanding of cyber risks and threats related to cyber attackers. | | | | | | * Foundation knowledge or awareness of ISMS standards such as ISO27001 and/or Cyber Security Essentials | | | | | | | |
| * Foundation knowledge of pulling system reports and log analysis | | | | | | * Excellent interpersonal skills, and good verbal and written and communication skills | | | | | | | |
| * Basic understanding of Agile methodology and practice | | | | | | * Basic knowledge of scripting and/or programming language such as python, powershell, BASH or KQL. | | | | | | | |
| * Desirable candidates should have computer and technical skills but do not need to have completed a technical, information security or similar degree. | | | | | |  | | | | | | | |
| Training offer | | | | | | | | | | | | | |
| We will fund the successful applicant to complete the CompTIA Cybersecurity Analyst (CySA+) certification or equivalent and they will also have access to official Microsoft training and a learning path in Pluralsight. | | | | | | | | | | | | | |
| L&Q Values | | | | | | | | | | | | | |
| These are our guiding principles. They describe how we deliver our mission and vision through our behaviours and actions. | | | | | | | | | | | | | |
| People | | | | | | | | | | | | | |
| • We care about the happiness and wellbeing of our customers and employees | | | | | | | | | | | | | |
| Passion | | | | | | | | | | | | | |
| • We approach everything with energy, drive, determination, and enthusiasm | | | | | | | | | | | | | |
| Inclusion | | | | | | | | | | | | | |
| • We draw strength from our differences and work collaboratively | | | | | | | | | | | | | |
| Responsibility | | | | | | | | | | | | | |
| • We own problems and deliver effective, lasting solutions | | | | | | | | | | | | | |
| Impact | | | | | | | | | | | | | |
| • We measure what we do by the difference we make | | | | | | | | | | | | | |
| Other | | | | | | | | | | | | | |
| * Commit to supporting L&Q’s environmental policy and social mission * I will comply with all L&Q Health and Safety policies and procedures and commit to working towards best practice in the control of health and safety risks | | | | | | | | | | | | | |