|  |  |  |  |
| --- | --- | --- | --- |
| **Job Title** | **Security Operations Analyst** | | |
| **Reports to** | **Cyber Security Programme Delivery Manager** | | |
| **Department** | **Technology** | | |
| **Job Family** | **Business Services** | **Level** | **3** |

|  |
| --- |
| **About the School** |
| At London Business School, we strive to have a profound impact on the way the world does business, and the way business impacts the world. Our departments work hard to ensure that we are continually delivering a world-class service, academic excellence and that our course offering maintains our place as a leading business school.  With thought-leading faculty and dynamic learning solutions, we empower both businesses and individuals by offering a transformational learning experience that will broaden their professional knowledge and global mindset. As well as offering postgraduate courses for the business leaders of the future, we run open and customised executive courses for professionals and corporate clients that help leaders identify the future focus and strategic direction of their businesses.  With London in our hearts, we draw from its status as a financial, entrepreneurial, and cultural hub to attract a diverse range of students and faculty, creating an abundance of opportunities to network with industry experts and alumni worldwide. |

|  |
| --- |
| **About the Department** |
| The LBS Technology department is responsible for delivery and supporting all digital technology solutions required for the effective running of London Business School.  We provide specialist capability in Service Delivery, Software Development, Digital Solutions Delivery, Teaching and Learning Technology, Platform integration, Data Management, Cyber Security, Project Delivery, Business Change and Enterprise Architecture.  Information security is a priority focus for Technology. We are committed to driving improvements across the full scope of our security capabilities to reduce the risk of business-impacting incidents and to ensure our information and systems are secured. |

|  |
| --- |
| **Job Purpose** |
| The Security Operations Analyst role is responsible for operating the security tooling, processes and procedures involved in monitoring and defending London Business School’s networks and systems.  The role is newly created to provide dedicated security operations resource within the Cyber Security team. |

|  |
| --- |
| **Key Areas of accountability and Key Performance Indicators (KPIs)** |
| **Key areas of accountability:**  **Delivery & Support**   * Perform security operations activities, in line with relevant policies and procedures. * Identify and recommend opportunities for improvements and enhancements. * Work collaboratively within the Information Security team and across wider Technology teams log and communicate risks and issues. * Participate in the development and enhancement of technical security policies and standards. * Support and participate in technical information security assurance activities. * Support the production of operational reports.   *Security Monitoring & Detection:*   * Proactively monitor London Business School’s suite of security tooling and external information sources to identify and detect threats. * Analyse and investigate security events and incidents to identify potential threats and vulnerabilities. * Maintain and tune security tooling alerts, detection rules and automated response. * Support system onboarding to security operations.   *Security Incident Response:*   * Support the definition, documentation and testing of security event and incident response playbooks. * Investigate and respond to security alerts, incidents, and breaches in a timely manner. * Provide support for security incident response. * Ensure all security incidents, risks and issues are logged and tracked to completion.   *Vulnerability Management:*   * Conduct security assessments and vulnerability scans to identify weaknesses and recommend remediation actions. * Ensure remediation activities are identified, assigned, coordinated, and tracked until completion, liaising across Technology teams as required.   *Threat Intelligence:*   * Maintain internal and external sources of information to feed into tooling to improve monitoring and detection. * Stay informed on the latest cybersecurity threats, trends, research, reports and good practice. * Collaborate across Technology to share threat intelligence and promote good practice. * Provide advice on emerging security threats. |

|  |
| --- |
| **Knowledge/Qualifications/Skills/Experience required** |
| * Bachelor’s degree in computer science, Information Security, or a related field (or equivalent work experience). * Proven experience working in a SOC or in a similar role. * Strong understanding of network protocols, cybersecurity principles, and threat landscapes. * Familiarity with SIEM tools and security technologies (e.g., Splunk, Palo Alto, FireEye). * Experience with incident response procedures and best practices. * Knowledge of security standards and frameworks (e.g., NIST, ISO 27001). * Excellent problem-solving and analytical skills. * Effective communication and teamwork abilities. * Relevant certifications such as CompTIA Security+, Certified Information Systems Security Professional (CISSP), or Certified Ethical Hacker (CEH) are a plus. * Advantageous – Engineering knowledge of Microsoft security tooling. |

|  |
| --- |
| **Resources including team management** |
| * None direct |

|  |  |
| --- | --- |
| **Staff** | None direct |
| **Budgets** | None direct |
| **Date Updated** | March 24 - FINAL |