LONDON BOROUGH OF REDBRIDGE
ROLE DESCRIPTION AND PERSON SPECIFICATION

Role Title:	Cyber Security Analyst		
Directorate:	Resources	**Grade:**	LBR 10
Department:	IT & Digital	**Hours/weeks:**	36 hours/52.14 weeks
Function:	Cyber Security and Information Governance	**Post number:**	S003246
Team:	Cyber Security	**Base/location:**	Lynton House / hybrid working, subject to Council policy
Reports to:	Head of Cyber and Information Governance		
Responsible for:	No direct reports. May coordinate managed security service providers, suppliers and contractors, and provide task leadership during incidents.		

Role and Context

Overall Role Purpose:	To protect Council services and information by monitoring, triaging and investigating cyber security events; coordinating proportionate incident response; managing vulnerabilities and security actions; and supporting security assurance, risk management and secure-by-design delivery. The role provides clear, evidence-based advice and works with the managed Security Operations Centre, IT teams, Information Governance, service owners and suppliers.
Role Context:	The Council operates a complex and changing digital estate and must protect essential public services and sensitive information. The postholder will work within the Council's cyber security governance, risk appetite, incident response arrangements and IT governance framework. The role will collaborate closely with Infrastructure, Architecture, Service Management, Information Governance, business continuity, Internal Audit and external security partners while retaining professional objectivity when assessing risk. The postholder will handle sensitive security information, maintain reliable records and escalate material risks, incidents and control weaknesses through agreed routes.

Key Accountabilities and Result Areas

Strategy and Planning	SFIA alignment: Information security; Threat intelligence; Risk management; Specialist advice (target levels to be confirmed at job evaluation). • Maintain current knowledge of threats, vulnerabilities and security good practice relevant to local government. • Support cyber risk assessments, control reviews, audit activity and evidence collection, including CAF, PSN, PCI DSS and other applicable assurance requirements. • Assess security implications of projects, suppliers, service designs and changes through the Council's IT governance and IT Compliance Agreement processes. • Maintain clear risk, exception and remediation records, escalating material or overdue issues. • Contribute to incident response, vulnerability management, awareness and resilience plans, exercises and lessons learned.
Operations and Support	SFIA alignment: Security operations; Incident management; Vulnerability assessment; Digital forensics (target levels to be confirmed at job evaluation). • Monitor and triage alerts and intelligence from the managed SOC, SIEM, endpoint, identity, email, network, cloud and vulnerability-management services. • Validate, investigate, contain and escalate suspected incidents in accordance with playbooks and delegated authority. • Preserve evidence and maintain accurate, time-sequenced incident records, decisions, communications and closure evidence. • Coordinate technical investigation and remediation with IT teams, suppliers, service owners, Information Governance and business continuity colleagues. • Operate the vulnerability-management lifecycle: validate findings, assess risk, assign ownership, track remediation, verify closure and escalate exceptions. • Review privileged access, configuration, logging and other control evidence where assigned. • Use threat intelligence, including relevant NCSC and local-government sources, to identify exposure and recommend proportionate action. • Participate in an agreed out-of-hours incident response or escalation rota where operationally required and contractually arranged.

Systems and Process Development and Improvement	SFIA alignment: Process improvement; Penetration testing coordination; Information assurance (target levels to be confirmed at job evaluation). • Maintain operational procedures, playbooks, knowledge articles, control records and security documentation. • Coordinate penetration tests and security assessments, ensuring findings have owners, target dates, evidence and retest outcomes. • Support secure-by-design reviews and verify that agreed security requirements are met before implementation or risk acceptance. • Improve use cases, alert quality, dashboards and reporting with the managed SOC and technical teams. • Analyse trends across incidents, vulnerabilities, phishing simulations, assurance findings and control exceptions to identify improvement priorities. • Create targeted guidance and awareness material, and support cyber exercises and lessons-learned reviews.
Communication and Partnership	SFIA alignment: Specialist advice; Stakeholder relationship management (target levels to be confirmed at job evaluation). • Communicate technical risk clearly to technical and non-technical audiences, distinguishing fact, assessment, recommendation and decision. • Build effective working relationships with IT, Information Governance, Audit, Procurement, HR, Communications, service owners, suppliers and external security partners. • Produce concise incident, vulnerability, assurance and performance reports for operational and governance forums. • Handle sensitive matters with discretion and share information only through authorised channels.
Performance and Standards	Manage and prioritise an evidence-based work plan across alerts, incidents, vulnerabilities, assurance actions, service requests and planned improvement activity. Meet agreed service levels, maintain accurate records, escalate blockers promptly and contribute to team resilience and continuous improvement.
Key Performance Outcomes	• Security alerts and incidents are triaged, recorded, escalated and closed within agreed priorities and service levels. • High-risk vulnerabilities and control weaknesses have accountable owners, target dates, evidence and verified outcomes. • Audit, CAF, PSN, penetration-testing and other assurance actions are progressed and evidenced. • Security monitoring coverage, use cases and data quality are reviewed and improved. • Reports are accurate, timely and actionable, with material risks and overdue actions escalated. • Exercises and incidents produce lessons that are tracked to evidenced closure.
Resource Management	Coordinates work with the managed SOC, security suppliers and occasional contractors. Responsible for appropriate use of assigned security tools, licences, evidence repositories and sensitive security information; no direct budget responsibility unless separately delegated.
Corporate Accountabilities	All employees of the Council should undertake and conduct their work with due regard to the corporate accountabilities (available on the Redbridge Council website). These include responsibilities for outcomes regarding equality, conduct, health & safety, data protection, safeguarding and customer care.
Flexibility	The key responsibilities and duties of the role are neither exclusive nor exhaustive. All workers are expected to operate flexibly to support delivery of services and from time to time will be required to undertake responsibilities outside the normal remit of role description as required by the line manager, which are broadly commensurate with the job level and scope of competence.

Person Specification Method of Assessment: A=application, I=interview, T=test Weighting: 3=most important, 2=least important		**A,I,T**	**Weighting**
Knowledge & Experience		I,T	3

Educational Ability	**Essential knowledge and experience:** • Practical security monitoring, alert triage and investigation using SIEM, endpoint, identity, email, network or cloud-security telemetry. • Incident handling, including evidence preservation, escalation, containment support, documentation and lessons learned. • Vulnerability-management processes, risk-based prioritisation, remediation tracking and verification. • Core security concepts covering identity and access, least privilege, logging, patching, network security, cloud security, malware, phishing and data protection. • Clear written reporting and communication of technical risk to different audiences. **Desirable experience:** • Microsoft 365/Azure security services, Intune, Splunk, Tenable or comparable technologies. • Working with a managed SOC, penetration-testing supplier or threat-intelligence service. • Public-sector assurance frameworks such as NCSC CAF, PSN, PCI DSS, ISO/IEC 27001 or the NHS Data Security and Protection Toolkit. • Secure-by-design, supplier assurance, business continuity exercises or cyber awareness activity.	A/I/T A/I/T A/I/T A/I/T A/I/T A/I/T A/I/T A/I/T A/I/T	3 3 3 3 3 2 2 2 2
Key Subject or Content Areas (inc: Desirable Qualifications)	CISSP / CISM or equivalent qualification ISO 27001 qualifications preferred.	A	2
Knowledge / Experience	Experience of using relevant monitoring and configuration management software including SCCM Splunk Intune Advanced understanding of data protection practice and GDPR.	A I	2
	Excellent problem-solving skills in technical and service delivery environments using logic, knowledge and sound processes to analyse information and apply solutions.	I	3
	Able to empathise with customers and understand their business needs. Committed to ensuring excellent customer care through the efficient use of resources.	I	3
	Able to influence customer expectations and their use of IT systems. Gains co-operation of colleagues from other teams in delivery of services and acceptance of security standards.	I	3
	A good team worker and able to establish rapport quickly with customers, colleagues and partners. Builds confident and effective working relationships at all levels.	I	3
	Able to prioritise work with minimal supervision, balance incidents and planned activity against deadlines, maintain accurate records and escalate competing priorities or resource constraints.	I	3
	Adaptable, receptive to new ideas, and willing and able to adjust to new demands and circumstances.	I	3

Additional selection criterion	Requirement	Assessment	
Analytical judgement	Can assess incomplete or conflicting technical evidence, determine urgency and recommend proportionate action without overstating certainty.	I / T	3
Incident response	Can explain a structured approach to triage, evidence preservation, containment, escalation, communication and recovery.	I / T	2
Vulnerability management	Can prioritise remediation using exploitability, exposure, asset criticality, business impact and compensating controls, and verify closure.	I / T	2
Communication	Can produce a concise written incident or risk briefing for both technical and senior audiences.	T	3

Ethics and confidentiality	Demonstrates integrity, discretion, appropriate challenge and awareness of legal and organisational boundaries.	A / I	3
Continuous improvement	Uses metrics, root-cause analysis and lessons learned to improve controls, playbooks and monitoring.	I	3

Corporate Behaviours	The Council has a set of behaviours that all employees are expected to deliver in the performance of their role. The behaviour framework can be found on the Council's intranet page, and these should be reflected in your application and the way you work. As part of an individual's personal development Redbridge expects employees of all levels to be continuously developing these core behaviours.	
Effective and Collaborative Team Working	To take responsibility for personal development and actively participate in all learning and development. To participate in the on-going development, implementation and monitoring of service plans. To support and contribute to service efficiency and improvement.	

Working Pattern and travel	Monday to Friday, 36 hours per week, normally between 8.00 am and 6.00 pm, subject to the Council's working arrangements. Occasional out-of-hours or weekend work may be required for incidents, testing or recovery activity. Any formal on-call or standby requirement, frequency and remuneration must be specified in the recruitment pack and contract.
Special Factors or Constraints	The postholder will have access to sensitive security, personnel and incident information and must maintain confidentiality, integrity, professional judgement and a clear audit trail. They must comply with Council policies on information handling, acceptable use, data protection, equality, health and safety, safeguarding and records management. Conflicts of interest and suspected misuse must be declared and escalated through approved routes.

Version:	2.0 – revised recruitment draft
Last Reviewed:	16/09/2026