West Midlands Combined Authority

Job Description

Job Title:	Cyber Security Manager
Directorate/Team:	Technology & Insight Directorate
Location:	16 Summer Lane or other site/location
Responsible to:	Head of Corporate IT
Responsible for:	A small security engineering team (e.g., Principal Cyber Security & Infrastructure Specialist; Senior Cyber Security Specialist) and associated suppliers/MSSPs
Key working relationships: (internal)	CTIO; BMU Lead (and Information Security & Integrity Manager); Enterprise Architect; Heads of Product/Data/Technology Systems & Infrastructure; Data Protection Officer/Information Governance; Audit; Legal; Procurement
Key working relationships: (external)	Auditors, Managed SOC/MSSP, pen-test providers, security vendors, assurance bodies

Purpose of the Post

Lead and mature WMCA's operational cyber security capability. Own the implementation and operation of security controls across hybrid cloud, workplace and infrastructure; deliver technical incident response and remediation; drive vulnerability closure and identity/endpoint hygiene; and provide audit-ready evidence into WMCA's assurance cadence. Work within the Information Security & Integrity Management policies and risk frameworks, and within Enterprise Architecture guardrails to drive a DevSecOps way of working into all BaU, product teams and change projects. Lead the operational relationship with WMCA's outsourced SOC, ensuring high-quality monitoring, alert triage, escalation handling, and threat intelligence consumption; validate SOC performance against SLAs/SLOs, drive continuous improvement, and ensure seamless integration with WMCA's internal incident response and vulnerability management processes.

Owns technical IAM enforcement and CE+/PCI technical controls evidence, runs out-of-hours response with SOC/MSSP and leads technical Disaster Recovery rehearsals aligned to information security and integrity policy and enterprise architecture guardrails. Works in partnership with the Information Security & Integrity Manager (ISIM) to achieve the organisation's information security objectives.

Accountabilities

- Operate security controls to defined Minimum Security Baselines and policies; meet SLA/SLOs for patching, vulnerability Mean Time To Remediate, identity hygiene and change success.
- Lead technical incident response (contain–eradicate–recover) and support ISIM with incident governance and reporting.
- Lead the technical Disaster Recovery posture for cyber incidents (runbooks, rehearsal/exercises, recovery validation), aligning with ISIM's BCP/DR requirements.
- Maintain security tooling (EPP/EDR, firewalls, email/web filtering, SIEM inputs, identity protections, posture/ASR rules) and ensure robust monitoring/alerting.
- Own technical enforcement of Identity & Access Management (e.g., conditional access, privileged access hygiene, risky-user reduction), maintain IAM hygiene KPIs, and implement ISIM's policy requirements in identity platforms.
- Provide and manage the technical control evidence for CE+ and PCI DSS, and deliver remediation of audit/assessment findings to agreed SLAs *(Information Security & Integrity Manager owns the programme and audit responses).*

- Provide operational evidence (metrics, logs, runbooks) into CAB and Business Management Unit assurance packs.
- Provide and manage technical control evidence for CE+ and PCI DSS and deliver remediation of audit/assessment findings to agreed SLAs; operate and harden in-scope controls (e.g., endpoint, identity, network, logging) in line with ISIM policy.
- Commission and technically coordinate penetration testing; own remediation.
- Manage a small security engineering team and suppliers; build skills, SOPs and reusable patterns.
- Contribute technical content to awareness and training led by ISIM.

Responsibilities

Strategic

- Translate policy/guardrails (ISIM/EA) into pragmatic technical patterns drawing on industry best practice.
- Shape the secure-by-default posture of platforms and devices; influence technical roadmaps.
- Establish a culture of internal peer review and challenge for cyber security practice across operational teams and engage external support and training to maintain a high standard of practice.
- Contribute to the organisation's Cyber and Resilience Strategy so as to support and enable overall organisational strategy and objectives
- Participate in regional collaboration initiatives such as the regional WARP and other instruments as required

People

- Build strong working relationships across T&I service areas, Corporate PMO, Service Desk, suppliers and operational teams and technical teams across the WMCA.
- Coach/line-manage engineers; provide vendor/supplier oversight; Rota management.
- Provide technical modules within the organisation-wide security awareness programme (labs/demos/playbooks), led by ISIM.
- Promote a culture of disciplined, evidence-driven continuous improvement.
- Lead the awareness and training plan; coach control owners on compliance.
- Build strong relationships across RUN/CHANGE.
- Work collaboratively with all colleagues and stakeholders to further common goals.
- Promote agile and Lean working practices across the directorate, including team ceremonies, retrospectives and continuous improvement cycles.
- Support capability-building by identifying skill gaps, utilisation patterns and upskilling needs.
- Create a culture of safety around the organisation's Information Security eco-system where blameless lessons learnt are rapidly embedded into continuous improvement cycles.

Operational

- Operate an out-of-hours/on-call rota for critical incident response and coordinate with the SOC/MSSP for 24×7 escalation and containment.
- Ingest threat intelligence from NCSC/ROCU/CiSP and SOC sources and convert it into tuned controls (detections, policies, hardening standards) and actionable changes, evidencing updates through BMU cadence.
- Run a pen-test intake and closure process: register findings, assign owners, track to SLA, report exceptions to ISIM/BMU, and evidence closure at CAB/change gates.
- Execute technical forensics under ISIM-owned chain-of-custody, preserving evidential integrity and supporting legal/IG processes.
- Run daily/weekly security ops cadence: vulnerability triage, patch windows, rule/review cycles.
- Lead post-incident technical Root Cause Analysis CA and feed lessons into Business Management Unit cycles.
- Ensure build-to-run security readiness for changes/releases.

Financial

- No direct budget responsibility, but Input to security/compliance budgets; optimise licence/usage

Other

- Publish and maintain KPI targets for patch compliance, vulnerability MTTR, identity risk reduction and change success; present trends and actions into BMU reviews and security governance.
- Operate effective matrix working between the Directorate and WMCA Corporate PMO to ensure effective project delivery, portfolio oversight, and financial monitoring.
- Ensure adherence to WMCA governance, HR, procurement and financial protocols.
- Support the BMU Lead in maintaining a high-quality operational environment, predictable workflows, and disciplined scheduling practices.
- Drive continuous improvement in operational processes, tools, and ways of working.
- Represent the WMCA in a professional manner.
- Undertake such tasks as may reasonably be expected commensurate with the scope and level of the role.

Person Specification

Candidates/post holders will be expected to demonstrate the following:	Essential / Desirable		How Evidenced?		
Experience	**E**	**D**	**A***	**I***	**T***
• Aligning to ISO 27001 in complex, multi-supplier environments.	x		x	x	
• Leading technical incident response and remediation.	x		x	x	
• Hybrid cloud security in Microsoft 365 / Azure.	x		x	x	
• Operating security controls at scale (firewalls, endpoint, identity, email/web, vulnerability/patch).	x		x	x	
• Establishing policies, MSBs, risk registers, DPIAs, and supplier security.	x		x	x	
• Commissioning pen tests and driving remediation.	x		x	x	
• Managing technical teams and suppliers	x		x	x	
• Experience working with operational, service, delivery or technology-related data.	x		x	x	
• Experience producing dashboards, reports or analytics for senior stakeholders.	x		x	x	
• Experience supporting continuous improvement or lessons-learned processes.	x		x	x	
• Experience of working in Agile, Lean or DevOps-aligned delivery practices (e.g., Kanban, flow metrics, sprint planning, CI/CD awareness).	x		x	x	
• Experience of working with CABs, release cycles or readiness reviews.	x		x	x	
• Experience working in or alongside portfolio-led environments with multiple concurrent projects or product teams.		x	x	x	
Skills / Knowledge	**E**	**D**	**A***	**I***	**T***
• Strong analytical ability, attention to detail and record-keeping discipline and ability to interpret operational data.	x		x	x	
• Understanding of enterprise architecture, service management, or technology asset management.	x		x	x	
• Strong grasp of NCSC guidance, MITRE ATT&CK, NIST CSF, secure configuration baselines.	x		x	x	
• Hands-on with EDR/EPP, SIEM inputs and SOC workflows (alert triage, escalation, tuning), identity protections, conditional access, and secure hardening practices.	x		x	x	
• Strong documentation and runbook discipline, excellent communication and influencing skills.	x		x	x	
• Proficiency with reporting and visualisation tools (e.g., Power BI, Excel, dashboarding platforms).	x		x	x	
• Understanding of performance frameworks (KPIs, OKRs, SLAs) and basic statistical concepts.	x		x	x	
• Ability to work with technical teams to gather and validate information.	x		x	x	
• Understanding of ITIL service metrics, delivery flow measures or DevOps telemetry.		x	x	x	

• Understanding of digital and technology delivery environments: software engineering, data pipelines, corporate IT operations, OT/public-realm systems.		x	x	x	
• Highly organised; strong attention to detail; excellent communication skills; strong problem-solving ability.		x	x	x	
• Familiarity with DevOps toolchains (e.g., Azure DevOps, Jira, GitHub boards, CI/CD pipelines).		x	x	x	
• Collaborative, diplomatic, and able to influence across organisational boundaries.	x		x	x	
• Proactive, organised, and comfortable managing multiple priorities.	x		x	x	
• Committed to continuous improvement and high standards of delivery.	x		x	x	
• Able to build trust and credibility with senior leaders and technical experts.	x		x	x	
• Ability to communicate complex information clearly to senior stakeholders.	x		x	x	
• Ability to interpret and report financial, performance and operational information	x		x	x	
Qualification / Education / Training	**E**	**D**	**A***	**I***	**T***
Evidence of relevant continuous professional development.	x		x		
Degree or equivalent experience; one or more of CISSP/CISM, AZ-500/SC-200+, or equivalent.	x		x		
ITIL Foundation; SANS/GIAC; cloud security certifications		x	x		
Qualifications in data analysis, service management, Agile/Lean, or continuous improvement (e.g., basic Lean/Six Sigma).		x	x		

***Key: A** = Application, **I** = Interview, **T** = Testing/Assessment

Core Expectations

Health, Safety & Wellbeing	All employees have a duty to take reasonable care for the health, safety, and wellbeing of themselves and of other persons who may be affected by their acts or omissions at work; and co-operate with their employer so far as is necessary to enable it to successfully discharge its own responsibilities in relation to health, safety, and wellbeing.
Equality & Diversity	Promote and champion equality and diversity in all aspects of the role.
Learning & Development	Participate in and take responsibility of any learning and development required to carry out this role effectively.
Performance Management	Actively engage in the performance management process and take responsibility for managing performance outcomes.
GDPR	Ensure the reasonable and proportionate protection, processing, sharing, and storing of WMCA information in accordance with the relevant legislation, corporate policies, and in the best interests of the data subjects (Data Protection/GDPR), the WMCA, our partners, and the West Midlands, in all aspects of the role.
Adherence to Policies	Be aware of and comply with all organisation policies.
Other	There may be a requirement to work outside normal office hours on occasion, including a requirement to work within stakeholder and partner offices within the WMCA constituent area on a regular basis.

Values

Our culture is underpinned by what we do and how we do it. Our behaviours outline the ways we need to work to deliver success, become truly inclusive, and make the organisation somewhere where everyone can give their best contribution.

Value	Competency	Behaviour
Collaborative	Team Focussed	Works as part of team, managing and leading.

	Service Driven	Customer, resident, and partner focussed.
Driven	Empowered & Accountable	Takes ownership and leads when needed.
	Performance Focused	Ambitious and going the extra mile.
Inclusive	'One Organisation' Mindset	Believe in each other's expertise.
	Open & Honest	We do what we say we are going to do.
Innovative	Forward Thinking	Embrace change and open to new possibilities.
	Problem Solving	Go for clear and simple whenever possible.

Additional Post Requirements									
Essential Car User		**Politically Restricted Post**		**Disclosure and Barring Service (DBS)**				**Vetting**	
Yes ☐	No ☐	Yes ☐	No ☐	Basic ☐	Standard ☐	Enhanced ☐	None ☐	Yes ☐	No ☐

Job Evaluation Details			
Date Evaluation Agreed	**JEP Reference**	**Grade**	**Job Family**