

Dataspire

A smiling man with a beard, wearing a green shirt, is pointing towards a screen in a meeting. He is surrounded by other people whose hands are visible on the table. The background is a blurred office setting. A large blue circular graphic is overlaid on the top right of the image.

Role Profile:

Senior Systems Operation Engineer

Since our inception, the Dataspire team have always been passionate about education, almost as much as we're crazy about IT.

Our focus has been simple: to work in partnership with schools of all sizes in creating dependable and high-performing IT environments which ensure staff have total confidence in using ICT to deliver outstanding learning outcomes for their students.

Key Information

Company Details:

Dataspire Solutions, Lowry Mill, Lees Street, Manchester, M27 6DB

Role Location:

Hybrid

Salary:

Competitive salary dependent on experience

Reporting into:

Head of Technical Services

To Apply:

Please send your CV and a brief cover letter to:

careers@dataspire.co.uk

Are you a senior operations engineer who thrives at the intersection of infrastructure resilience and cybersecurity? If you want to step away from reactive break/fix support and take ownership of the NOC and SOC methodologies that keep hundreds of schools secure, online, and compliant, this could be the role for you.

About the role

As a Senior Systems Operations Engineer, you will be the functional and technical lead for our Systems Management team, operating as a combined NOC/SOC function. You will own the roadmaps, standards, and operational processes across our infrastructure monitoring, enterprise backup, and security operations platforms.

You will not just be resolving tickets; you will be analysing threat vectors, tuning alert thresholds, and building the automation that reduces alert fatigue for the whole team. You will act as the Major Incident Manager during critical outages or security events and will work closely with our Solutions Design and Implementation teams to ensure every new customer environment is built "operations-ready."

Key responsibilities

- Lead the operation, configuration, and evolution of Dataspire's NOC/SOC tooling (infrastructure monitoring, backup, and security platforms), defining intelligent alerting thresholds to minimize noise.
- Own incident, problem, and change processes, acting as the primary coordinator and escalation point for Major Incidents (e.g., widespread outages, ransomware containment).
- Provide technical leadership on proactive security operations (SOC), driving MFA rollouts, rigorous patching cadences, vulnerability scan remediations, and disaster recovery readiness.
- Define, author, and maintain the runbooks, standard operating procedures (SOPs), and incident response playbooks for the team to ensure consistent, NCSC-aligned execution.
- Analyse trends in system alerts, threat telemetry, and capacity to recommend and deploy automated remediation scripts, materially reducing manual effort.
- Work with Solutions Design and Implementation to mandate that new solutions include appropriate monitoring coverage and backup controls prior to operational handover.
- Mentor Systems Operations Engineers, building their capability in both network operations and proactive security hunting, and contribute to technical training for the wider business.

Technologies you'll operate and manage

- **Monitoring & Observability (NOC):** Infrastructure and SaaS monitoring tools (N-Able, Zabbix or similar) ensuring high availability and capacity management.
- **Security Operations (SOC):** Managing secure remote access (VPN, RDS), vulnerability tracking, MFA enforcement, and ensuring compliance with NCSC security baselines.
- **Backup & Disaster Recovery:** Enterprise backup, immutable storage, and DR platforms (e.g., Redstor), rigorously enforcing the 3-2-1 rule.
- **Remote Management & Automation:** RMM tools, service desk software, and custom scripting to drive auto-remediation.
- **Core Infrastructure:** Windows Server, Virtualisation (Hyper-V, VMware), and Identity (Active Directory, Azure AD/Entra ID).
- **Networking:** Operating and monitoring edge networks, firewalls, and enterprise Wi-Fi (HPE Aruba, Cisco).

What we're looking for

- A strong background in NOC, SOC, or senior infrastructure operations roles within an MSP or similar enterprise environment.
- Extensive hands-on responsibility for monitoring, enterprise backup (e.g., Veeam, Commvault, Redstor), and security tooling at scale.
- Demonstrable experience designing operational processes and automation (scripting) to improve system reliability, accelerate incident response, and reduce manual toil.
- A calm, structured, and authoritative approach to Major Incident Management and complex root-cause analysis (RCA).
- A "documentation-first" mindset: you enjoy writing clear incident playbooks, runbooks, and sharing knowledge with others.
- A collaborative approach: comfortable acting as an escalation point and working as part of our "One Team" across Service and Implementation.
- **Nice to have:** An understanding of education-sector risk profiles, school safeguarding requirements, or DfE/NCSC cyber guidelines.

Why this role matters

Our mission is to create dependable, high-performing IT environments that give teachers confidence in using technology and help young people access outstanding learning experiences. In this role, your work is the invisible safety net that keeps schools running. By ensuring backups are watertight, security is proactive, and outages are prevented, you directly protect teaching and learning time. If you are motivated by the idea of using your operational and security expertise to make a tangible difference in education, this is the role for you.