Respected. Included. Performing at our Best.

RESPECT • OPENNESS • COLLABORATION
PERFORMANCE • CREATIVITY

GSOC Analyst with Specialism x 2

Role title	Group Security Operations Center (GSOC) Operations Analyst - Specialisms	Salary Range	£37,485 - £44,100
Function	Chief Operating Officer	Role Level Range	4-5 (inc on call payment)
Base Location	Flexible – Herdus House, West Cumbria, Hinton House, Warrington; London or Harwell, Oxfordshire Hybrid working available with 40% of time in an NDA office	Role Type	Permanent
Reports to	GSOC Service Leads	Closing Date	20th August 2026

The opportunity and your impact

Reporting to GSOC Service Leads, these 2 roles are responsible for supporting the GSOC team across a range of cyber security operations activities, with each postholder providing GSOC analyst capability and inclusion in an on-call Rota, while contributing to a specialism aligned to business need across the group. The specialisms may include:

- SOC operations and incident response
- Detection engineering and analytics
- Threat hunting and threat-informed defence
- AI-enabled augmentation, automation and workflow optimisation

The roles will contribute to the ongoing delivery and continuous improvement of GSOC services, while remaining flexible to support operational priorities, incidents and emerging threats across the NDA and its Operating Companies.

These roles will work closely with GSOC personnel and wider cyber security functions to perform and improve monitoring, triage, investigation, detection capability, threat-informed analysis, workflow efficiency, reporting, and documentation. This includes supporting the effective use of telemetry, analytical techniques and, where appropriate, controlled automation or AI-assisted approaches to enhance GSOC operations and support to the GSOC capability overall. All roles will require participation in an on-call Rota.

What you'll do

- Support delivery of core GSOC capabilities including SOC analysis, threat hunting, detection engineering, AI augmentation / automation and OT support
- Support personnel engaged in providing Cyber Security Operations capabilities and services within the GSOC
- Provide technical and analytical support to GSOC staff and NDA Operating Companies in relation to monitoring, investigations, incidents, and specialist activities
- Monitor, triage, investigate and respond to security alerts and incidents, including participation in an on-call Rota for out of hours events / incidents
- Support the development, testing and tuning of detection logic, search queries, analytical content and monitoring use cases across GSOC tooling
- Support proactive and hypothesis-led investigations using telemetry, threat intelligence, behavioural analysis and available monitoring platforms
- Contribute to the onboarding, quality, correlation and effective use of security telemetry and assets across GSOC customers
- Support the use of workflow improvements, automation and AI-assisted techniques to improve triage, enrichment, reporting and operational efficiency, ensuring appropriate human oversight and governance
- Support the translation of threat intelligence, adversary behaviours, red teaming and authorised testing activity into improved detection, monitoring and response outcomes
- Support multi operating company cyber security operational incidents when required
- Support provision of advice and guidance across the NDA Group in relation to GSOC operational specialism
- Support continuous improvement of processes, playbooks, procedures and supporting documentation within GSOC, ensuring outputs are clear, controlled and auditable
- Support other capabilities within the GSOC as and when required

The successful candidate(s) will be able to demonstrate:

- Remaining calm under pressure
- Working methodically and following complex defined procedures and operational processes
- Investigating complex problems and identifying effective solutions using technical and analytical approaches
- Collaborating with other specialists across the group in operational, technical and assurance functions
- Interpreting outputs from monitoring systems and analytical tooling to distinguish malicious or insecure behaviour from benign activity both in hours and out of hours, responding or escalating as required
- Identifying, categorising and managing incidents, and supporting their investigation and resolution

- Analysing unexpected network, endpoint, identity or system events and supporting appropriate response actions
- Managing the accurate and timely sharing of important operational information
- Contributing to incident response processes, detection documentation, playbooks and continuous improvement activities
- Applying an understanding of attacker behaviours, threat intelligence or adversary techniques to improve defensive outcomes
- Supporting the effective use of tools and techniques such as SIEM, EDR/XDR, query languages, telemetry analysis, workflow automation and dashboards
- Operating within a regulated, safety-conscious environment with appropriate governance, documentation and assurance

Your background, skills, and strengths

- At least 1 - 2 years' experience within Cyber Security Operations or Information Security
- Experience in one or more areas such as SOC analysis, incident response, detection engineering, threat hunting, security analytics, automation or cyber threat intelligence
- Practical experience using cyber security monitoring technologies and interpreting alerts and telemetry
- Familiarity with query languages such as KQL, SQL or equivalent
- Ability to contribute to detection logic, analytical outputs, workflows and technical documentation
- Awareness of threat frameworks (e.g. MITRE ATT&CK) and their application
- Strong analytical, communication and collaboration skills
- Ability to work methodically and manage competing priorities
- Awareness of governance, assurance and controlled working practices in a regulated environment
- Awareness of cyber-physical or critical infrastructure environments would be advantageous
- Relevant degree, apprenticeship or equivalent experience in Cyber Security, Information Security, Computer Science or related discipline
- Desirable registration with a recognised professional body (e.g. IISP, BCS, ISC2, ISACA)
- Relevant certifications aligned to cyber security operations, detection, analytics or automation would be advantageous
- Ability to obtain SC clearance

What we offer:

- Generous performance based annual bonus scheme.
- Defined benefit Civil Service pension scheme (please find more information here).
- 30 days annual leave per year, plus 8 statutory public and bank holidays (pro-rata for part-time employees).
- A range of family-friendly flexible working options.

Respected. Included. Performing at our Best.

RESPECT • OPENNESS • COLLABORATION
PERFORMANCE • CREATIVITY

We will give priority consideration to employees within the NDA group who are currently at risk or progressing through the redeployment process.

All applicants from the NDA Group of companies may be eligible for protection of certain elements of their T&Cs when voluntarily taking up employment with another NDA Group Company. If successful in your application, your existing Group Employer's HR team will collaborate with the new Group Employer's HR team to ensure that the appropriate protections are implemented into your contract offer. For further details, please contact a member of your current HR team.

We value the unique differences that each of our colleagues bring to work every day and are committed to creating an environment where everyone feels respected, included and able to perform at their best. At NDA, we are committed to creating a workplace that is diverse and inclusive. We value the diversity of our people and actively seek to have a workforce that represents the rich diversity of the communities we support.

Currently, we are underrepresented in some areas, and would particularly welcome applicants from Women, Black, Asian and Ethnic Minorities, LGBTQ+ and candidates who have a disability.

NDA is a member of the disability confident scheme, when requested we will make reasonable adjustments to the recruitment process and we guarantee to interview all candidates who have a disability who meet all of the essential criteria for the vacancy.

We are happy to discuss flexible working. We will also make workplace adjustments for disabled employees if these are needed to help them perform at their best in the role, and we are happy to discuss this once a job offer has been made.

disability confident LEADER

PROUD TO SUPPORT THE SUNFLOWER
FOR INDIVIDUALS WITH HIDDEN DISABILITIES

To apply:

Find out more about the NDA group and other available opportunities by visiting www.ndagroup.careers

We welcome applications from external candidates who are not employed by the NDA Group (including ASWs, Graduates, Apprentices and CSWs). Please note that applicants from the internal pool will be given priority consideration. External applications will be considered once the internal pool has been exhausted.