Senior SOC Analyst

We are looking for a passionate and dedicated Senior SOC Analyst with experience in a similar cloud solutions or technical environment to work within our fast paced, growing team. You will be at the forefront of helping to build and design a new managed security product and function based on the Microsoft Azure and Defender stack.

Our 24x7 Security Operations Centre, detects, and investigates security threats affecting corporate and customer platforms gathered from disparate sources, including from cyber threat sensors and threat intelligence data.

Required Skills & Experience

- 3 Years+ Infra/Network/Security experience
- 2 Years+ SOC Analyst experience
- Understanding of Cyber Security Principles
- Experience of DLP, WAF, IPS, Web Proxy techs
- Experience of threat hunting
- Ability to obtain & hold security clearance

Additional (not essential) Skills & Experience

- Relevant security qualification or degree
- Responsibility for managing security technologies
- Experience with Microsoft Defender or Azure Sentinel

Responsibilities & Duties

- Work as part of a 24*7 SOC via on-call rota.
- Develop and maintain incident response playbooks for common threat and incident types, ensuring that colleagues are formally kept aware of any changes.
- Triage and manage Security Events and Incidents reported by both internal and external sources through their lifecycle, from identification through to mitigation, within defined SLA's.
- Support the wider business in the handling of major Security Incidents.
- Proactively hunting for threats through analysis and correlation of event and flow data from a variety of sources.
- Identify and drive continual monitoring and response improvements, including use case, content and playbooks, that will lead to a reduction in Mean Time To Detect (MTTD) and Mean Time to Respond (MTTR) metrics.
- Perform root cause analysis of all incidents.
- Manage, monitor and maintain Security Operations managed Security Controls such as SIEM, DLP, SWG and WAF appliances.
- Handle incoming Security Service Requests & Queries on behalf of the wider business.
- Ensure that personal and colleague Information Security knowledge is always current and up to date with latest threats and mitigation actions.
- Contribute to daily technical stand-ups.

- Produce and deliver daily and weekly metrics and reports.

The reasons to work for us:

Our Warrington based office has everything you would expect from a growing tech company, free snacks, stylish breakout spaces and people you will enjoy spending time with... and that's not even including the office dog, who can beat us all at football!

Benefits & Extras:

- Fun office environment with breakout spaces
- 24 days holiday per year
- Free fruit, snacks, and drinks
- Regular team lunches
- Perkbox – employee discounts, recognition cards and competitions
- Cycle to work scheme
- Techscheme
- Private Healthcare
- Dental cover
- Free eye tests and money towards glasses/contact lenses
- Employee Assistance Programme
- Contributory Pension

If this role has you bouncing in your seat drop us your CV, we'd love to chat.