Senior Cyber Security Analyst | Full Time/Hybrid Working | Competitive Package

Senior Cyber Security Analyst

A Wilmslow based IT Service Provider is seeking for a Senior Cyber Security Analyst to join their team working within an MSP aspiring to become an MSSP. You will be committed to delivering, developing and improving professional services that have security engrained within each and every service they offer.

This role ensures the investment in security services and technology are effectively administered and supported on a daily basis with defined daily, weekly and monthly activities that are needed to ensure all services are delivered optimally and efficiently in line with contractual commitments and customer expectations.

General

- Day to day monitoring and administration of security controls around tooling solutions and cloud-based systems such as Office 365, AWS, Azure.
- Day to day monitoring of SIEM, data protection, vulnerability scanning, threat detection and Intelligence, working in conjunction with appropriate technology and technology partners.
- Monitor Frontline and customer security services to ensure that patching, security controls and mechanisms are operating effectively – investigate issues and escalate through the Service Desk toolset.
- Assist in developing, maturing and managing the existing operational processes for run / play books to be created or automated where possible.
- Assist in delivering security reviews and management metrics to ensure integrity, confidentiality, and availability.
- Provide analysis, review, and creation of monthly reports for Frontline and customers.
- Proposes improvements within the scope of the security operations that will lead to automation, standardisation, and consolidation for ease of support and maintenance.
- Create working relationships with business stakeholders to deliver and enhance security services.
- Take ownership in obtaining information, evidence and data required to diagnose and resolve complex problems.
- Proactively analyse trends and reports to highlight potential problems, maintain and enhance service.
- Flexible member of the security operations team to provide knowledge, assistance, and advice with other team members.
- Maintain awareness of technical and service developments, taking the initiative to extend own knowledge to learn about products, technologies, and techniques to deliver enhanced services.
- Monitoring of events and alerts from multiple technologies to detect potential malicious activity.
- Responsible for carrying out analysis and triage of cyber security events.
- Taking ownership to identify and assess the appropriate outcome and response to an event.
- Clear and concise communication and collaboration when responding to events through remediation.
- To identify, escalate and debate all risks to the business, by analysing events/metrics and escalation data, identify patterns and trends on high-risk controls and proactively suggest, develop and implement enhancements to reduce risk.

Roles and Responsibilities

- Event / Ticket Management
- Escalation
- Tooling
- Reporting and Performance
- Knowledge and Documentation

Experience

- 3-5 years' experience working within an IT Security / Cyber Security function (preferably an MSP / MSSP)
- 3-5 experience working within an IT service environment (preferably an MSP / MSSP)
- Experience working with a variety of network tooling and complex network infrastructure.
- Experience working in an environment adhering to and/or accredited industry standards/frameworks such as ISO27001/27002, Cyber Essentials (Plus), NIST, SOC2
- Experience in delivery and development of Cyber Security tooling and process.
- Experience with Microsoft Security Tooling such as Defender suite
- Experience with advanced threat and/or vulnerability detection technologies

Desired Skills / Certifications

- Sound understanding of information security risk assessment and mitigation.
- Understanding of Cloud IaaS, PaaS and SaaS (ideally Azure), web application security (OWASP Top 10) and database technology.
- Certified Ethical Hacker Certification (CEH)
- Offensive Security Certified Professional Certification (OSCP)
- Certified Penetration Tester & Certified Expert Penetration Tester (CPT & CEPT)
- GIAC Security Essentials Certification (GSEC)
- Systems Security Certified Practitioner (SSCP)
- CompTIA Security+
- CompTIA Network+
- CompTIA Advanced Security Practitioner (CASP+)
- Degree in information technology, computer science or similar, or with equivalent industry qualifications in cyber security.

Benefits

- Company enrolled benefits package.
- Salary Sacrifice Cycle to Work Scheme
- Employee Assistance Programme
- 22 standard days annual leave plus UK bank holidays.
- 1 additional annual leave day on your birthday.
- 2 additional annual leave days entitlement at Christmas.
- Pension Scheme after 3 months of service.
- Pool Table, Massage Facilities and Next-Gen console on-site.
- Company laptop.
- Employee of the Month bonus scheme of £500 if you are successful
- Referral fee of £1,000 if successful
- Funded training in line with Company and personal objectives

Vacancy Information:

- Location: Wilmslow/ Hybrid Working
- Salary range: Competitive
- Job type: Permanent
- Job Section: Information Technology
- Working Hours: Full-Time

Senior Cyber Security Analyst, IT Security, Cyber Security Function, Tooling, Cyber Security, Permanent, Wilmslow